Information Disclosure Statement

New U.S. Patent Application for
INTEGRATED SECURITY INFORMATION MANAGEMENT SYSTEM AND METHOD
Our Ref. No.: P03EB013/US/jy

Reference No.:

(1) KR Laid-Open No. 2001-67966

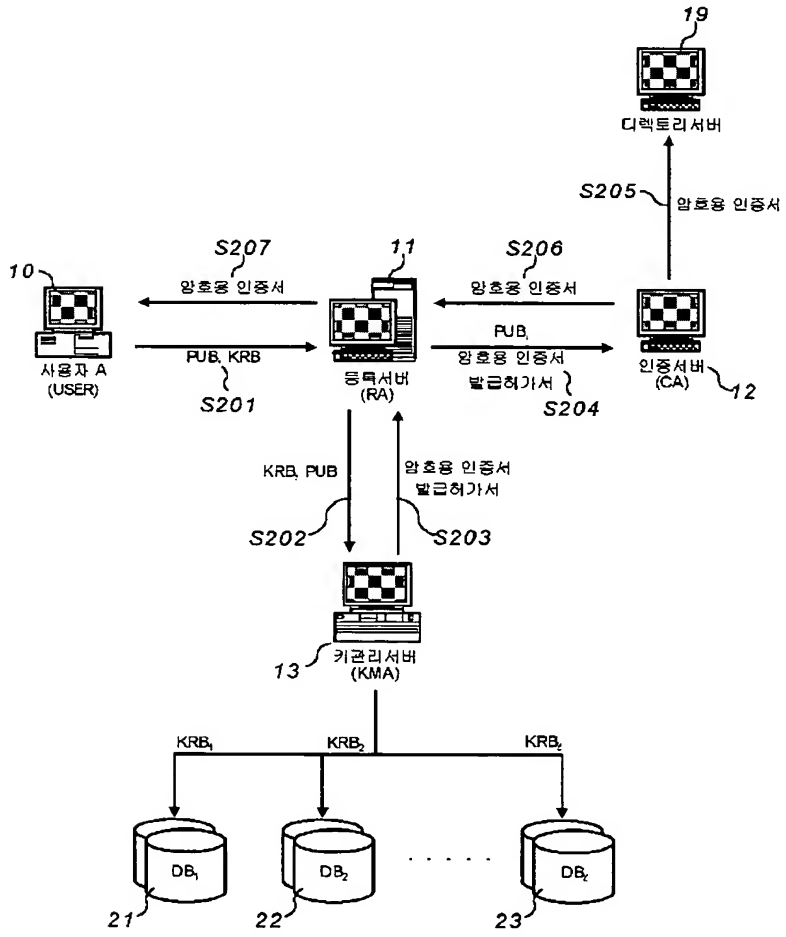
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020010067966 (43) Publication.Date. 20010713
(21) Application No.1020010019279 (22) Application Date. 20010411
(51) IPC Code:
H04L 9/08

(71) Applicant:
KOREA INFORMATION SECURITY AGENCY
(72) Inventor:
KIM, JI YEON
KIM, SEUNG JU
KWON, HYEON JO
LEE, HONG SEOP
PARK, HAE RYONG
(30) Priority:

(54) Title of Invention
PKI-BASED COMMERCIAL KEY ENTRUSTING METHOD AND SYSTEM

Representative drawing



(57) Abstract:

PURPOSE: A PKI-based commercial key entrusting method and system are provided which provides PKI-roaming service without changing a system and guarantees perfect forward secrecy for a key management server managing a key recovery server.

CONSTITUTION: A user A(10) generates a pair of password private key and public key and creates a key recovery block to transmit the key recovery block together with the public key to a registration server (11) in the first step(S201). The registration server transmits the key recovery block and public key to a key managing server(13) at the second step(S202). The key managing server sends a password authentication note issuance permit to the registration server at the third step(S203). The registration server shows the permit to an authentication server(12) and requests a password authentication note with respect to the public key at the fourth step(S204). The authentication server issues the password authentication note and opens the authentication note to a directory server (1) at the fifth step(S205), and transmits the authentication note to the registration server at the sixth step(S206). The registration server delivers the password authentication note to the user A at the seventh step(S207).

관리번호: 1P20030300 (마킹)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 9/08

(11) 공개번호 특2001-0067966
(43) 공개일자 2001년07월13일

(21) 출원번호 10-2001-0019279
(22) 출원일자 2001년04월11일

(71) 출원인 한국 정보 보호 센터
서울특별시 서초구 서초동 1321-6 동아타워 5층

(72) 발명자 김지연
서울특별시송파구잠실6동장미아파트29-1008

김승주
서울특별시종로구혜화동26-6

권현조
서울특별시성동구마장동466-1

박해룡
광주광역시광산구우산동1046-4

이홍섭
서울특별시성북구돈암동616한신아파트101-1006

(74) 대리인 원태영

심사청구 : 있음

(54) 피케이아이 기반의 상업용 키위탁 방법 및 시스템

요약

본 발명은 공개키 기반의 인프라와 연동되면서 사용자와 정부의 요구 사항을 동시에 충족시키는 실용적인 키위탁 시스템 기술을 개시한다.

본 발명에 따른 키위탁 기술은 시스템 변경 없이 피케이아이(Public Key Infrastructure; PKI)-로밍(roaming) 서비스를 제공하고, 키복구 서버를 관리하는 키관리 서버에 완전 순방향 비밀성(perfect forward secrecy)을 보장함으로써 안전성을 제고한다. 본 발명에 따른 키위탁 기술이 강제적 시스템으로 적용될 경우에도 사용자의 프라이버시를 최대한 보장하는 이점이 있다.

대표도

도4a

색인어

공개키, 비밀키, PKI, 키위탁 시스템, Key Escrow, Key Recovery.

명세서

도면의 간단한 설명

도1a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 넷스케이프사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면.

도1b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 넷스케이프사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면.

도2a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 베리사인사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면.

도2b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 베리사인사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면.

도3a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 인트러스트사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면.

도3b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 인트러스트사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면.

도4a를 참조하면, 본 발명에 따른 키위탁 시스템의 제1 실시예를 나타낸 것으로서, RSA(Ron Rivest, Adi Shamir, Leonard Adleman) 기반의 (n,n)-상업용 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도4b는 본 발명의 제1 실시예에 따른 RSA 기반의 (n,n)-상업용 키위탁 시스템의 키복구 과정을 나타낸 도면.

도5는 본 발명에 따른 키위탁 시스템의 제2 실시예를 나타낸 것으로서, RSA 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도6은 본 발명에 따른 키위탁 시스템의 제3 실시예를 나타낸 것으로서, RSA 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도7a는 본 발명에 따른 키위탁 시스템의 제4 실시예를 나타낸 것으로서, 디피-헬만(Diffie-Hellman) 기반의 (n,n)-상업용 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도7b는 본 발명의 제4 실시예에 따른 디피-헬만 기반의 (n,n)-상업적 키위탁 시스템의 키복구 과정을 나타낸 도면.

도8은 본 발명에 따른 키위탁 시스템의 제5 실시예를 나타낸 것으로서, 디피-헬만 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도9는 본 발명의 제6 실시예를 나타낸 것으로서, 디피-헬만 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도10a는 본 발명의 제7 실시예를 나타낸 것으로서, 디피-헬만 기반의 (t,n)-상업용 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도10b는 본 발명의 제7 실시예를 나타낸 것으로서, 디피-헬만 기반의 (t,n)-상업용 키위탁 시스템의 키복구 과정을 나타낸 도면.

도11은 본 발명의 제8 실시예를 나타낸 것으로, 디피-헬만 기반의 (t,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

도12는 본 발명의 제9 실시예를 나타낸 것으로, 디피-헬만 기반의 (t,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면.

<도면의 주요 부분에 대한 부호의 설명>

10	:	사용자(USER)
11	:	등록 서버(RA; Registration Authority)
12	:	인증 서버(CA; Certification Authority)
13	:	키관리 서버(KMA; Key Management Authority)
14, 15, 16	:	키복구 서버(KRA; Key Recovery Agent)
21, 22, 23	:	데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 PKI(Public Key Infrastructure) 기반의 키위탁 시스템 기술에 관한 것으로, 특히 사용자의 프라이버시(privacy) 보호와 정부의 법집행 능력을 보장이라는 상반된 목적을 동시에 충족할 수 있는 키위탁 시스템 및 방법에 관한 것이다.

컴퓨터 통신 기술의 발달로 현대인들은 언제 어디서나 각종 데이터를 주고받으며 정보통신 시대를 살아가고 있다. 그런데, 유무선 통신망을 통한 전자상거래, 금융거래 등의 정보통신 산업이 급속히 팽창함에 따라서, 데이터 암호화 기술의 중요성이 한층 배가되고 있다.

암호는 온라인(on-line) 메시지(message)를 부호화(encoding)하는 기술을 의미하며, 적절한 부호(code) 또는 키(key)를 갖고 있는 자만이 복호화하여 해독할 수 있게 된다. 이와 같은, 암호의 사용은 정보의 누출 및 오용을 방지하고 상대의 신원 확인을 가능하게 함으로써, 온라인 상에서의 전자상거래나 전자계약을 가능하게 하는 등 많은 장점을 가지고 있다. 그러나, 암호는 본래 가지고 있는 키관리의 어려움 때문에 다음과 같은 문제가 발생할 수 있다.

첫째로, 키의 분실이나 손실로 인하여 사용자가 자신의 키 또는 평문(plain text; 암호화가 되지 않은 메시지)에 접근할 수 없는 경우가 종종 발생한다. 이 경우에는 자신이 적법한 소유자임에도 불구하고 자신의 정보에 접근을 할 수 없으므로 예기치 않은 손실을 초래할 수 있다.

둘째로, 기업의 입장에서 볼 때에 암호가 오용됨으로써 잠재적 위협을 발생시킬 수 있다. 즉, 사업장에서 피고용인이 중요한 정보를 암호화하고 키를 담보로 하여 금품을 요구할 수도 있으며, 키의 도난이나 손상 등의 위협이 항상 존재하게 된다.

셋째로, 국가와 같은 공공 기관이 범죄 수사 등의 적법한 이유로 키 또는 평문에 접근하여야 할 필요성

이 발생한 경우에 야기될 수 있는 문제점이다. 즉, 범죄자는 암호문을 사용함으로써 합법적 수사를 방해할 수도 있게 된다.

전술한 첫 번째 문제점인 개인 사용자가 겪을 수 있는 키의 분실 또는 손실 문제는 키 백업(key back-up) 서비스 등을 제공하는 상업용 키위탁 시스템을 이용함으로써 해결할 수 있다. 또한, 기업 또는 국가의 입장에서 발생될 수 있는 상기 문제점은 기업의 보안 정책이나 국가 차원의 정책으로 사용되는 강제적 키위탁 시스템으로 해결될 수 있다.

전술한 암호 사용의 역기능을 해결하는 대안으로서, 암호 사용에 대한 법률 규제, 발표되지 않은 트랩도어(trapdoor)가 있는 암호 방식의 채택, 또는 모든 암호 사용에 정부가 개입하는 등의 방법이 소개되고 있으나, 현재 지지를 받고 있는 대표적 방안은 키위탁 시스템(key escrow system)이다.

키위탁 시스템은 암호문의 소유자(일반적인 암호 시스템에서 키를 소유한 사람)가 아닐지라도, 사전에 약속된 어떤 특정한 조건하에서 허가된 사람에게 복호가 가능한 능력을 제공하는 암호 시스템이라 정의할 수 있다. 여기서, 미리 약속된 조건이란 암호가 나쁜 목적으로 사용되었을 경우의 법집행 권한 확보를 위한 허가일 수도 있고, 데이터 암호용 키를 상실하였을 경우가 될 수도 있다.

이와 같은 PKI 기반의 키위탁 시스템의 대표적 기술로서 넷스케이프 (Netscape)사와 베리사인(Verisign)사 및 인트러스트(Entrust)사의 기술이 알려져 있다. 이하에서는, 종래 PKI 기반의 키위탁 시스템의 문제점을 이해하기 위하여 위에서 언급한 3개 회사의 기술을 차례로 살펴보기로 한다.

우선, PKI 기반의 키위탁 시스템의 구성 객체는 다음과 같다. 사용자(user)란 PKI 기반의 상업용 키위탁 시스템의 서비스를 이용하는 객체를 의미하며, 사용자가 인증서 발행을 요청할 때에 전자 서명용 인증서 및 암호용 인증서를 생성하여 발행하여 주는 인증 서버가 존재한다.

또한, 등록 서버는 인증 서버가 인증서(certificate)를 발행하기에 앞서서 암호용 인증서 발급을 요청한 사용자를 확인하고 그에 대한 등록 업무를 수행한다.

한편, 키복구 과정을 위하여 사용자의 비밀키를 백업하여 저장하여 두게 되는데, 사용자의 키복구 요청시에 키복구를 수행하는 키관리 서버와 키관리 서버에게 키복구 정보를 제공하는 다수의 키복구 서버가 구성된다.

즉, 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템은 사용자, 등록 서버, 인증 서버, 키관리 서버와 다수의 키복구 서버로 구성됨을 특징으로 한다. 여기서, 키복구 서버는 키복구에 필요한 정보를 제공하는 객체 또는 관련 운영자이므로 단일 객체를 사용하는 경우 키복구 권한의 남용이 우려될 수 있으므로, 복수개 KRA_1, KRA_2, …, KRA_n를 구성하는 것이 통용되고 있다.

또한, 키관리 서버는 키복구 서버를 관리하는 중앙 관리 서버의 역할을 수행하게 된다.

도1a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 넷스케이프사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면이다. 도1a에 도시된 PKI 기반의 상업용 키위탁 시스템은 '넷스케이프 인증 관리 시스템 운영자 설명서 버전 4.1(Netscape certificate management system administrator's guide version 4.1)' http://docs.iplanet.com/docs/manuals/cms/41/adm_guide/contents. html에 개시되어 있다.

도1a를 참조하면, 사용자 A(10)는 암호용 개인키 S_A와 공개키 P_A를 생성하고, 자신의 암호용 개인키 S_A를 키관리 서버(KMA; 13; 넷스케이프사에서는 '데이터복구 관리자'라 칭함)의 전송용 공개키 P_{KMA}로 암호화 $E_{P_{KMA}}(S_A)$한 후, 자신의 암호용 공개키 P_A와 함께 $E_{P_{KMA}}(S_A)$를 등록 서버(RA; 11)에 전송한다(단계 S100).

이어서, 등록 서버(RA; 11)는 사용자 확인 절차를 수행한 후, 사용자(10)의 암호용 공개키 P_A와 암호화된 사용자의 개인키 $E_{P_{KMA}}(S_A)$를 키관리 서버(KMA; 13)에 키위탁을 위하여 전송한다(단계 S101). 키관리 서버(KMA; 13)는 자신의 전송용 개인키 S_{KMA}를 이용하여 암호화된 사용자의 개인키를 복호화 후에 사용자의 암호용 공개키 P_A와 대응되는지를 검사한다.

이 때에, 복호화된 사용자의 개인키와 사용자의 암호용 공개키 P_A가 대응이 되는 경우, 자신의 저장용 공개키 P'_{KMA}로써 사용자의 암호용 개인키 S_A를 $E_{P'_{KMA}}(S_A)$로 암호화한 후 데이터베이스(17)에 저장한다(단계 S102).

한편, 키관리 서버(KMA; 13)의 저장용 개인키는 소프트웨어 또는 하드웨어 토큰에 저장되며 PIN을 통해 접근이 가능하다. 키관리 서버(KMA; 13)는 PIN을 (m,n)- 비밀 분산 알고리즘(단, m < n)을 사용하여 n개의 조각으로 조각낸 후에 n개의 키복구 서버 (KRA; 14, 15, 17) 키복구 관련 운영자의 패스워드로 암호화하여 보관한다.

다시 도1a를 참조하면, 키관리 서버(KMA; 13)는 사용자(10)의 암호용 개인키를 위탁한 후, 키관리 서버(13)는 등록 서버(RA; 11)에게 사용자의 암호용 개인키 S_A의 위탁이 완료되었음을 알리는 메시지를 자신의 전송용 개인키로 전자 서명하여 전송한다(단계 S104).

이어서, 등록 서버(RA; 11)는 서명된 메시지를 검증한 후, 인증 서버(CA; 12)에게 인증서 발급을 요청한다(단계 S105). 이에 따라, 인증 서버(CA; 12)는 사용자에 대한 암호용 인증서를 발급한 후 등록 서버(RA; 11)에게 전송한다(단계 S106). 이어서, 등록 서버(RA; 11)는 암호용 인증서를 사용자 A(10)에게 전송한다(단계 S107).

도1b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 넷스케이프사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면이다. 도1b를 참조하면, 사용자 A(10)로부터 암호용 개인키에 대한 복구 요청(단계 S120)을 수신한 키관리 서버(KMA; 13)는 자신의 키복구 관련 정책에 적합한지를 검사한 후에 적합하다면 이에 대한 확인 메시지를 n명의 키복구 서버(KRA; 14, 16)에 전송한다(단계 S121).

한편, 키복구 서버(KRA)들은 확인 메시지를 검사한 후 자신들의 식별 정보 와 함께 패스워드 $PSWD_1$, $PSWD_2$, …, $PSWD_n$을 키관리 서버(KMA; 13)에 안전하게 전송한다(단계 S122). 이어서, 키관리 서버(KMA; 13)는 m명의 키복구 서버(KRA)의 패스워드를 이용하여 PIN을 재구성한 후에 자신의 저장용 개인키에 접근한다.

이 저장용 개인키를 이용하여 데이터베이스에 저장되어 있는 사용자의 암호용 개인키를 복구한다. 키관리 서버(KMA; 13)는 복구된 사용자의 암호용 개인키를 안전하게 사용자 A(10)에게 전송한다(단계 S123).

도2a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 베리사인사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면이다. 베리사인사가 개시하고 있는 PKI 기반의 상업용 키위탁 시스템 기술은 'Onsite Key Management Service Administrator's Guide', http://www.verisign.com에 상세히 기술되어 있다.

도2a를 참조하면, 베리사인사의 키위탁 시스템은 전술한 넷스케이프사의 기술과 달리 사용자 A(10)의 개인키 및 공개키 쌍을 키관리 서버(KMA; 13, 베리사인사에서는 'Key Manager'라 칭함)가 생성하는 것을 특징으로 하고 있다. 이를 상세히 살펴보면 다음과 같다. 사용자 A(10)가 등록 서버(RA; 11)에 암호용 인증서 발급을 요청하면(단계 S130), 등록 서버 (RA; 11)는 사용자 A(10)의 암호용 인증서 발급 요청을 키관리 서버(KMA; 13)에 전송한다(단계 S131).

한편, 인증서 발급 요청을 수신한 키관리 서버(KMA; 13)는 사용자 A(10)의 암호용 개인키/공개키 쌍과 함께 3-DES키를 생성한다. 이어서, 키복구 레코드 (KRR; Key Recovery Record)와 키복구 블럭(KRB; Key Recovery Block)을 다음과 같이 생성한다. 즉, 키복구 레코드는 $KRR \quad E_K(PRI)$ 이고, 키복구 블럭 (KRB)은 $KRB \quad E_{P_{KRA}}(K)$ 이다. 여기서, K는 3-DES 키이고, PRI는 사용자의 암호용 개인키이고 P_{KRA}는 키복구 서버(KRA; 14)의 공개키이다.

한편, 키관리 서버(KMA; 13)는 생성한 키복구 레코드와 키복구 블럭을 사용자 개인 식별 정보와 함께 데이터베이스(17)에 저장한 후, 3-DES 키는 소거한다. 이어서, 키관리 서버(KMA; 13)는 인증 서버(CA; 12)에게 사용자의 인증서 발급을 요청하고(단계 S133), 인증 서버(CA; 12)는 사용자 암호용 인증서를 발급한 후 키관리 서버 (KMA; 13)에 전송한다(단계 S134). 이어서, 키관리 서버(KMA; 13)는 암호용 개인키와 암호용 인증서를 사용자 A(10)에게 안전하게 전송한다. 그리고 난 후에 사용자 암호용 개인키를 소거한다.

도2b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 베리사인사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면이다. 도2b를 참조하면, 사용자 A(10)가 키관리 서버(KMA; 13)에게 자신의 암호용 개인키 복구를 요청하는 경우(단계 S140), 키관리 서버(KMA; 13)는 데이터베이스(17) 검색을 통하여 사용자의 키복구 블럭을 검색한다(단계 S141). 이러한 작업을 수행하기 위해서는 두 명의 키 관리 서버 운영자의 PIN이 필요하다.

검색된 키복구 블럭과 키복구 요청서를 키복구 서버(KRA; 14)에 안전하게 전송한다. 키복구 서버(KRA; 14)는 키복구 요청서를 확인한 후, 자신의 개인키를 이용하여 키복구 블럭으로부터 3-DES 키를 복호화한다. 한편, 복호화된 3-DES 키는 키관리 서버(13)에 안전하게 전송된다.

이어서, 키관리 서버(KMA; 13)는 키복구 서버(KRA; 14)로부터 수신한 3-DES 키를 이용하여 키복구 레코드로부터 사용자의 암호용 개인키 S_A를 복구한 후 사용자에게 안전하게 전송한다(단계 S144).

도3a는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 인트러스트사가 개시하고 있는 키위탁 과정의 일처리 흐름을 나타낸 도면이다. 종래 기술에 따라 인트러스트사가 개시하고 있는 기술은 'Administering Entrust/PKI 5.0 on UNIX'에 상술되어 있다.

도3a를 참조하면, 사용자 A(10)는 등록 서버(RA; 11)에게 암호용 인증서 발급을 요청한다(단계 S150). 등록 서버(RA; 11)는 사용자 A(10)의 암호용 인증서 발급 요청을 인증 서버(CA; 12)에 전송한다(단계 S151). 한편, 인증서 발급 요청을 수신한 인증 서버(CA; 12)는 사용자 A(10)의 암호용 개인키 및 공개키 쌍을 생성한 후, 공개키에 대한 암호용 인증서를 생성한다.

사용자의 암호용 개인키/공개키 쌍과 인증서는 CAST-128 또는 3-DES 알고리즘으로 암호화되어 데이터베이스(17)에 저장된다(단계 S152). 한편, 인증 서버 (12)는 등록 서버(11)를 통해(단계 S153), 개인키와 암호용 인증서를 안전하게 사용자 A(10)에게 전송한다(단계 S154).

도3b는 종래 기술에 따른 PKI 기반의 상업용 키위탁 시스템으로서, 인트러스트사가 개시하고 있는 키복구 과정의 일처리 흐름을 나타낸 도면이다. 도3b를 참조하면, 키위탁 시스템의 키복구를 위하여 사용자 A(10)가 등록 서버(RA; 11)에 자신의 암호용 개인키의 복구를 요구하고(단계 S160), 등록 서버(RA; 11)는 사용자 A(10)의 암호용 개인키 복구 요청을 인증 서버(CA; 12)에게 전송한다(단계 S161).

이 때에, 인증 서버(CA; 12)는 데이터베이스(17)를 검색하여 암호화되어 저장되어 있는 사용자의 암호용 개인키를 복호화한다(단계 S162). 한편, 복구 과정 수행 시에 관련 운영자의 패스워드가 필요하며, 복구 과정에 참여하는 운영자의 수는 보안 정책에 따라 결정될 수 있도록 하고 있다. 이어서, 인증 서버(CA; 12)는 복호화된 사용자 암호용 개인키를 등록 서버(RA; 11)를 통해(단계 S163) 사용자 A(10)에게 전송한다(단계 S164).

이상에서, 대표적 종래 기술로서 넷스케이프사, 베리사인사 및 인트러스트사의 PKI 기반의 키위탁 기술을 상술하였다. 그런데, 전술한 베리사인사와 인트러스트사의 모델의 경우에는 사용자가 아닌 각각의 키관리 서버와 인증 서버가 사용자의 암호용 개인키를 생성하게 되므로, 키복구 과정이 아닌 키생성 과정에서부터 사용자의 암호용 개인키가 제3자에 노출되는 보안 문제점이 있다.

또한, 종래 기술로서 넷스케이프사 모델의 경우에도 위탁되는 개인키와 공개키의 대응성을 검사하기 위하여 키관리 서버의 전송용 키를 이용하여 사용자의 개인키가 암호화되어 전송되기 때문에, 키복구 과정이 아닌 키위탁 과정에서 키관리 서버에게 개인키가 노출되는 위험이 도사리고 있다.

더욱이, 넷스케이프사와 인트러스트사 모델의 경우 위탁된 사용자의 키는 그 를 관리하는 서버의 관련 키(넷스케이프사의 경우는 키관리 서버의 저장용 키, 인트러스트사의 경우는 인증 서버의 CAST-128 또는 3-DES 키)로 암호화되어 데이터베이스에 저장되므로 그 키를 별도로 안전하게 관리하여야 하는 부담과 함께, 이것이 일단 공개되면 데이터베이스에 저장된 사용자의 암호용 개인키는 노출되게 되는 문제점을 지니게 된다.

특히, 전술한 베리사인사 모델의 경우에, 키복구 서버는 키복구 블럭으로부터 복호화한 3-DES 키를 키관리 서버에게 안전하게 전송하기 위하여 CRS (Certificate Request Syntax) 프로토콜을 이용하므로, 키관리 서버는 CRS 프로토콜을 위한 키를 별도로 안전하게 관리하여야 하는 부담이 있다.

또한, 전술한 넷스케이프사, 베리사인사 및 인트러스트사의 모델의 경우에, 주기적으로 데이터베이스를 백업함으로써 장애 허용성(fault tolerance)을 보장할 수 있으나, 단일 데이터베이스에 저장됨으로 인해 불순한 자로부터 해킹 등의 공격 목표가 되기 쉽다.

발명이 이루고자하는 기술적 과제

따라서, 본 발명의 제1 목적은 기존의 PKI와 상호 연동이 되면서 실용적인 키위탁 시스템 기술을 제공하는데 있다.

본 발명의 제2 목적은 상업용 키위탁 시스템으로 활용되는 경우 활성화를 위하여 키 백업 기능 이외에 PKI-로밍 서비스와 같은 부가 서비스를 제공하는 키위탁 시스템을 제공하는데 있다. 여기서, PKI-로밍 서비스란 임의 클라이언트(client) 터미널에서도 패스워드(password)를 이용하여 비밀키를 내려받은(download) 다음, 그 정보를 이용하여 사용자가 PKI 기반 서비스를 이용하도록 하는 기술로서, 무선 인터넷과 같은 환경에서 사용자에게 이동성과 편리성을 제공하게 된다.

본 발명의 제3 목적은 상기 제2 목적에 부가하여, 합법적 접근권이 보장되는 PKI 기반의 키위탁 시스템 및 방법을 제공하는데 있다. 즉, 본 발명은 사용자 또는 법원 등의 키복구 요청이 없는 한 키관리 서버 및 키복구 서버가 사용자 암호용 개인키에 접근할 수 없는 키위탁 시스템 기술을 제공하는데 목적을 두고 있다.

본 발명의 제4 목적은 상기 제2 목적에 부가하여, 실용성 및 완전 순방향 비밀성을 보장하는 키위탁 시스템 기술을 제공하는데 있다. 상업용 키위탁 시스템 설계 시에 있어서, 키복구 서버 외에 이들을 관리하기 위한 별도의 중앙 관리 서버 (예를 들어, 키관리 서버)를 두는 것이 실용적이 될 수 있다.

여기서, 본 발명의 제4 목적을 완전 순방향 비밀성을 제공하는데 둔다함은 중앙 관리 서버의 긴 주기의 개인키(long-term private key)가 노출된다고 하더라도 이것이 위탁된 사용자 키의 안전성에 영향을 미치지 않음을 의미하는 것으로서, 중앙 관리 서버인 키관리 서버는 위탁되는 사용자의 암호용 키 관련 정보가 집중되는 곳이므로 이러한 성질은 매우 중요하다.

본 발명의 제5 목적은 상기 제2 목적에 부가하여, 키관리 서버 및 키복구 서버가 키복구 과정에서 사용자의 암호용 개인키를 알아낼 수 없는, 즉 은닉성 (blindness)이 제공되는 키위탁 시스템 기술 및 방법을 제공하는데 있다.

본 발명의 제6 목적은 상기 제2 목적에 부가하여, 저장되어 있는 사용자 위탁키에 대한 가용성이 증대되고, 키복구 정보 저장 장소의 장애 허용 기능이 제공되는 키위탁 시스템 기술을 제공하는데 있다.

본 발명의 제7 목적은 상기 제2 목적에 부가하여, 소프트웨어적으로 구현 가능한 키위탁 시스템 기술을 제공하는데 있다. 정보 보안의 중요성이 증가하면서, 키위탁 시스템은 누구나 쉽게 사용할 수 있어야 하므로 합리적인 가격으로 제공되어야 하며 높은 품질과 성능을 갖는 것이 바람직하다. 성능이 좋은 고품질의 키위탁 시스템은 탬퍼프루프(tamperproof)를 제공하는 하드웨어로 제작되어야 하지만, 본 발명은 경제성과 추후 전자상거래의 활용성 등을 고려하여 소프트웨어로 구현되는 것을 목적으로 한다.

본 발명의 제8 목적은 강제적 키위탁 시스템으로 활용되는 경우에도 사용자의 프라이버시가 최대한 보장되는 키위탁 시스템 기술을 제공하는데 있다.

본 발명의 제9 목적은 상기 제8 목적에 부가하여, 키복구 권한을 분산함으로써 키복구에 대한 사용자 신뢰성을 제고하고, 한 서버에 집중되어 공격 목표가 되는 것을 방지하는 키위탁 시스템 기술을 제공하는데 있다.

본 발명의 제10 목적은 상기 제8 목적에 부가하여 대량 감청을 방지할 수 있는 키위탁 시스템 기술을 제공하는데 있다.

발명의 구성 및 작용

상기 목적을 달성하기 위하여, 본 발명은 PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하는 사용자가 자신의 암호용 개인키/공개키 쌍을 생성하는 단계; 상기 사용자가 자신의 패스워드를 사용하여 상기 개인키를 암호화하는 단계; 상기 사용자가 n개의 키복구 서버의 공개키를 이용하여 키복구 블럭을 생성하는 단계; 상기 사용자가 상기 키복구 블럭과 공개키를 등록 서버에 전송하는 단계; 상기 등록 서버가

상기 키복구 블럭과 공개키를 키관리 서버에게 전송하는 단계; 상기 키관리 서버가 상기 수신된 키복구 블럭을 (m, ℓ)-비밀 분산 알고리즘(단, m < ℓ)을 사용하여 ℓ개의 조각으로 분할한 후, 각각의 조각을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스에 각각 나누어 저장하고, 상기 키복구 블럭을 소거하는 단계; 상기 키관리 서버가 상기 등록 서버에게 암호용 인증서 발급 허가서를 전송하는 단계; 상기 등록 서버가 인증 서버에게 상기 암호용 인증서 발급 허가서를 제시하고 사용자의 암호용 공개키에 대한 암호용 인증서를 요청하는 단계; 상기 인증 서버가 암호용 인증서를 발급하고, 디렉토리 서버에 상기 사용자의 암호용 인증서를 공개하고 상기 등록 서버에게 전송하는 단계; 및 상기 등록 서버가 상기 암호용 인증서를 상기 사용자에게 전송하는 단계를 포함하는 PKI 기반의 키위탁 시스템의 키생성 및 위탁 방법을 제공한다.

이하에서는, 첨부 도면 도4 내지 도12를 참조하여 본 발명에 따른 키위탁 시스템의 양호한 실시예를 상세히 설명한다.

도4는 본 발명에 따른 키위탁 시스템의 제1 실시예를 나타낸 것으로서, RSA 기반의 상업용 키위탁 시스템의 키생성 및 키위탁 과정과 키복구 과정을 각각 도4a와 도4b에 나타내고 있다.

도4a를 참조하면, 본 발명의 제1 실시예에 따른 RSA 기반의 (n,n) 상업용 키위탁 시스템의 키생성 및 키위탁 과정이 도시되어 있다. 이하에서 사용되는 기호를 먼저 설명하면 다음과 같다. 본 발명에서 패스워드(PWD)는 PKI-로밍 서비스를 위한 사용자 A의 패스워드를 의미한다.

또한, VER은 PKI-로밍 서비스를 위하여 키관리 서버에 등록된 사용자 A의 패스워드 확인자이다. 한편, KRB는 사용자 A에 대한 키복구 블럭을 나타낸다. 이하, 발명의 상세한 설명에서 (e_i, N_i)는 제i번째 키복구 서버(KRA_i)의 암호용 RSA 공개키이다. 단, $N_1 < N_2 < \cdots < N_i < \cdots < N_n$이다. 한편, d_i는 제i번째 키복구 서버 (KRA_i)의 복호용 RSA 개인키이다.

사용자 A(10)는 자신의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고, 사용자 A(10)는 KRB를 아래와 같이 생성하여 PUB과 함께 등록 서버(RA; 11)에 전송한다(단계 S201). 사용자 A(10)는 개인키 PRI를 자신의 패스워드 PWD로 암호화한다.

즉, $E_{PWD}(PRI)$를 계산한다. 이어서, 사용자는 자신이 원하는 키복구 기관의 공개키를 가지고 암호화를 하게 되며, KRB는 $KRB = (\cdots((C^{e_1} \bmod N_1)^{e_2} \bmod N_2)\cdots)^{e_n} \bmod N_n$의 식으로부터 연산된다. 다시 도4a를 참조하면, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 KRB와 PUB을 전송한다(단계 S202).

한편, 키관리 서버(KMA; 13)는 KRB를 (m, ℓ)-비밀 분산 알고리즘(단, m < ℓ)을 사용하여 ℓ개로 조각낸 후, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스 DB_1(21), DB_2(22), …, DB_ℓ(23)에 각각 나누어 저장한다.

이 때에, 저장이 완료되면, KRB는 소거된다. 이어서, 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 암호용 인증서 발급 허가서를 전송하게 되며(단계 S203), 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)의 암호용 인증서 발급 허가서를 제시한 후, 사용자 A(10)의 암호용 공개키 PUB에 대한 암호용 인증서를 요청한다(단계 S204).

이에 인증 서버(CA; 12)는 암호용 인증서를 발급한 후, 디렉토리 서버(19)에 사용자 A(10)의 암호용 인증서를 공개하고(단계 S205), 등록 서버(RA; 11)에게 암호용 인증서를 전송한다(단계 S206). 이어서, 등록 서버(RA; 11)는 사용자 A(10)에 암호용 인증서를 전송한다(단계 S207).

도4b는 본 발명의 제1 실시예에 따른 RSA 기반의 (n,n) 상업용 키위탁 시스템의 키복구 과정을 나타낸 도면이다. 도4b를 참조하면, 사용자 A(10)는 키관리 서버(KMA; 13)에게 자신의 암호용 개인키 복구를 요청한다(단계 S210). 본 발명에 따른 키관리 서버(KMA; 13)는 사용자 A(10)를 확인한 후에 데이터베이스 검색을 통하여 A에 대한 ℓ개의 키복구 블럭 조각 중 m개의 키복구 블럭 조각 KRB_1, KRB_2, …, KRB_m을 취합하고, (m, ℓ)-비밀 분산 알고리즘을 이용하여 KRB를 재구성한다.

본 발명에 따른 양호한 실시예로서, 키관리 서버(KMA; 13)는 다음 과정을 통하여 사용자 A(10)의 암호화된 개인키 $E_{PWD}(PRI)$를 복구한다. 즉, 키관리 서버(KMA; 13)는 은닉 인자(blind factor) r(단, 0 < r < N_1)을 랜덤하게 선택한 후, KRB'을 $KRB' = KRB \cdot (\cdots((r^{e_1} \bmod N_1)^{e_2} \bmod N_2)\cdots)^{e_n} \bmod N_n$의 식으로부터 계산하여, 암호용 개인키복구 요청서와 함께 제n번째 키복구 서버(KRA_n)에게 전송한다(단계 S211).

이어서, 제(n-1)번째 키복구 서버로부터 제1 키복구 서버까지 KRA_{n-1}, KRA_{n-2}, …, KRA_2, KRA_1(단계 S212부터 단계 S215까지)의 순서로 수신 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행한다. 이를 다시 수식으로 표현하면 다음과 같다.

$$KRA_n : KRB'_{(n)} = (KRB')^{d_n} \bmod N_n$$

$$KRA_{n-1} : KRB'_{(n-1)} = (KRB'_{(n)})^{d_{n-1}} \bmod N_{n-1}$$

$$KRA_2 : KRB'_{(2)} = (KRB'_{(3)})^{d_2} \bmod N_2$$

$$KRA_1 : KRB'_{(1)} = (KRB'_{(2)})^{d_1} \bmod N_1 = E_{PWD}(PRI) \cdot r \bmod N_1$$

한편, 제1번째 키복구 서버(KRA_1; 14)는 $KRB'_{(1)}$을 계산하여 키관리 서버 (KMA; 13)에게 다시 전송한다(단계 S216). 이어서, 키관리 서버(KMA; 13)는 $KRB'_{(1)}/r \bmod N_1$을 계산하여 $C_j = E_{PWD_j}(PRI_j)$를 복구한다.

한편, 사용자 A(10)의 패스워드 확인자를 소지한 키관리 서버(KMA; 13)는 복구된 사용자 A(10)의 $E_{PWD_j}(PRI)$를 패스워드 기반 다운로드 프로토콜을 이용하여 안전하게 사용자 A(10)에게 전송한다(단계 S217).

도5는 본 발명에 따른 키위탁 시스템의 제2 실시예를 나타낸 것으로서, RSA 기반의 강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 전술한 본 발명의 제1 실시예에 따른 상업용 키위탁 시스템의 경우에는 사용자의 입장에서 볼 때에 자신의 키가 복구되거나 또는 키가 복구되지 않는 것이 사용자에 달려 있게 되므로, 위탁되는 사용자의 키복구 블럭에 대한 정당성을 검증하는 절차가 불필요하다.

그러나, 상업용 키위탁 시스템이 아닌 대량 감청 방지 기능을 갖는 강제적 키위탁 시스템으로 활용되는 경우에는, 등록 서버가 위탁되는 사용자의 키복구 블럭에 대해 정당성을 검증하는 과정이 필요하게 된다. 즉, 기업주 또는 국가의 입장에서 사용자의 키복구 블럭이 정당성을 구비하고 있는지 여부를 검증하는 과정이 필요하면, 이에 대한 고려가 본 발명의 제2 실시예에 반영되어 있다.

그런데, 사용자의 키복구 블럭에 대한 정당성 검증을 위해 사용자의 개인키가 키관리 서버에게 공개되는 것은 개인키 노출로 인하여 사용자의 프라이버시를 해하게 되고 나아가 안전성에 위협이 될 수 있으므로, 종래의 넷스케이프사의 방식과는 다른 새로운 기술이 본 발명의 제2 실시예에 의해 개시된다.

따라서, 본 발명의 제2 실시예는 컷앤츄즈(cut-and-choose) 방식을 적용함으로써, 사용자의 키복구 블럭에 대한 정당성을 검증하면서도 사용자 개인키가 노출되지 않는 방식을 제시하고 있다. 도5를 참조하면, 사용자 A(10)는 s개의 패스워드 PWD_j(단, j = 1, …, s)를 생성하고, 이에 대응하는 s개의 패스워드 확인자 VER_j(단, j = 1, …, s)를 키관리 서버(KMA; 13)에 등록한다(단계 S221).

사용자 A(10)는 s개의 암호용 개인키/공개키 쌍(PRI_j, PUB_j)을 생성한다. 즉, 사용자 A(10)는 암호용 개인키 PRI_1, PRI_2, …, PRI_s와 공개키 쌍 PUB_1, PUB_2, …, PUB_s를 생성한다. 이어서, 사용자 A(10)는 개인키 PRI_j를 자신의 패스워드 PWD_j로 암호화한다(단, j = 1, …, s).

즉, $C_j = E_{PWD_j}(PRI_j)$(단, j= 1, …, s)를 계산한다. 이 때에, 긴급 감청이 필요한 키위탁 시스템으로 활용하고자 하는 경우에는, 사용자가 KRB를 생성하는 단계에서 PWD를 이용한 암호화 과정을 수행하지 않는다. 또한, s개의 키복구 블럭 (KRB_j)을 $KRB_j = (\cdots((C_j^{e_1} \bmod N_1)^{e_2} \bmod N_2)\cdots)^{e_n} \bmod N_n$의 식을 이용하여 생성하여, 공개키 PUB_j(단, j = 1, …, s)와 함께 등록 서버(RA; 11)에 전송한다(단계 S222).

s개의 KRB_j를(단, j = 1, …, s)와 PUB_j(단, j = 1, …, s)를 수신한 등록 서버(RA; 11)는 난수 k를 1 ≤k ≤s의 범위에서 선택하여 사용자에게 전송한다(단계 S223). 사용자 A(10)는 KRB_k를 제외한 (s-1) 개의 나머지 KRB_j를 오픈(open)한다. 즉, PWD_j, PRI_j(단, ∀j ≠k, 1 ≤k ≤s)를 등록 서버(RA; 11)에 전송한다(단계 S224).

이 때에, 본 발명에 따른 양호한 실시예로서 s의 크기에 따라 보안 강도를 조절하는 것이 가능하게 되며, 해쉬 함수를 이용하여 비대화형 방식으로 설계할 수 있다. 한편, 사용자 A(10)로부터 k값에 대응된 KRB_k를 제외한 나머지 (s-1)개의 KRB_j를 전송받은 등록 서버(RA; 11)는 PRI_j와 PUB_j의 대응성 및 KRB_j의 정당성을 다음의 식을 사용하여 검사한다(단, ∀j ≠k, 1 ≤k ≤s).

$$KRB_j \stackrel{?}{=} (\cdots((C_j^{e_1} \bmod N_1)^{e_2} \bmod N_2)\cdots)^{e_n} \bmod N_n$$

(단, ∀j ≠k, 1 ≤j ≤s)

상기 단계에서 PRI_j와 PUB_j의 대응성 및 KRB_j(단, ∀j ≠k, 1 ≤j ≤s)의 정당성이 검증되면, j = k인 경우에 대해서도 대응성 및 정당성이 검증된 것으로 간주하고, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 KRB = KRB_k와 PUB = PUB_k을 전송한다(단계 S225). 단계 S226 내지 단계 S230은 본 발명의 제1 실시예의 과정과 동일하다.

도6은 본 발명에 따른 키위탁 시스템의 제3 실시예를 나타낸 것으로서, RSA 기반의 강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 본 발명의 제3 실시예는 보다 실용적이며, 섀도우(shadow) 공개키 공격에도 안전한, 강력한 강제적 키위탁 시스템을 설계하고자 하는 경우, 키관리

서버(KMA; 13)가 사용자의 개인키/공개키 쌍을 생성한 후 패스워드 PWD로 암호화하여 사용자에게 전송하는 방식을 개시하고 있다.

도6을 참조하면, 사용자 A(10)는 등록 서버(RA; 11)에게 암호용 인증서 발급을 요청한다(단계 S231). 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 이를 다시 전송한다(단계 S232). 한편, 키관리 서버(KMA; 13)는 사용자 A(10)의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고, 키복구 블럭(KRB)을 아래와 같이 생성하여, 데이터베이스(21, 22, 23)에 분산 저장한다.

우선, 키관리 서버(13)는 사용자의 개인키(PRI)를 패스워드(PWD)로 암호화한다. 즉, $E_{PWD}(PRI)$를 계산한다. 그리고, PRI를 소거한다. 이 때에, 키관리 서버(KMA; 13)에는 사용자 A(10)의 PWD가 사전에 등록되어 있다고 가정한다. 이어서, KRB를 아래의 수학식 6을 이용하여 계산한다.

$$KRB = (\cdots(((\cdot)^{e_1} \bmod N_1)^{e_2} \bmod N_2)\cdots)^{e_n} \bmod N_n$$

또한, 키관리 서버(KMA; 13)는 (m, ℓ)-비밀 분산 알고리즘 (단, m < ℓ)을 사용하여 KRB를 ℓ개의 조각으로 조각낸 후에, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스 DB_1(21), DB_2(22), …, DB_ℓ(23)에 각각 나누어 저장한다. 이 때에, 저장이 완료되면 KRB는 소거된다.

이어서, 본 발명에 따른 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 '암호용 인증서 발급 허가서' 및 (C, PUB)를 전송하고(단계 S233), 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)로부터 전송된 '암호용 인증서 발급 허가서'를 제시하고 사용자 A(10)의 암호용 공개키 PUB에 대한 암호용 인증서를 요청한다(단계 S234).

이어서, 인증 서버(CA; 12)는 암호용 인증서를 발급한 후 디렉토리 서버(19)에 사용자 A(10)의 암호용 인증서를 공개하고(단계 S235), 등록 서버(RA; 11)에게 암호용 인증서를 전송한다(단계 S236). 마지막으로, 등록 서버(RA; 11)는 암호용 인증서와 C를 사용자 A(10)에게 전송한다(단계 S237).

본 발명의 제2 실시예에 따른 강제적 키위탁 시스템의 경우에는 도4b에 나타낸 키복구 방식을 사용하여 위탁된 사용자 개인키를 복구할 수 있으며, 이 경우에는 키관리 서버가 사용자 패스워드에 대한 사전 공격(dictionary attack)을 통해 사용자의 암호용 개인키 PRI를 복구할 수 있다.

본 발명의 제3 실시예에 따른 강제적 키위탁 시스템 기술은 도4b에 나타낸 키복구 방식을 사용하여 위탁키를 복구할 수 있으며, 이 경우에는 키관리 서버는 자신이 가지고 있던 사용자의 패스워드를 이용하여 사용자의 암호용 개인키 PRI를 복구한다.

이하에서는, 본 발명에 따른 키위탁 시스템과 종래 기술에서 언급한 3개 회사의 키위탁 시스템 기술을 비교하면서, 본 발명의 특징을 설명하기로 한다.

		넷스케이프 모델 (종래 기술)	베리사인 모델 (종래 기술)	인트러스트모델 (종래 기술)	제안 모델 (본 발명)
상업용	합법적 접근권 보장	X	X	X	0
	실용성 및 완전 순방향 비밀성	X	X	X	0
	은닉성	X	X	X	0
	키복구 정보 저장 장소의 장애 허용성	△	△	△	0
	S/W로 구현가능	0	0	0	0
	부가서비스	-	PKI-로밍서비스	PKI-로밍서비스	PKI-로밍서비스
강제적	키복구 권한의 분산	△	△	△ (보안 정책에 따름)	0
	대량 감청 방지	X	X	X	0

본 발명에서는 사용자의 암호용 개인키는 사용자만이 아는 패스워드로 암호화되고, 이것은 다시 키복구 서버의 공개키로 재 암호화되어 전송되므로, 합법적 접근권이 보장된다.

더욱이, 본 발명의 제2 실시예로서 강제적 키위탁 시스템의 경우에서도, 위탁되는 사용자의 개인키에 대한 정당성을 검증하기 위하여 컷앤츄즈 기법이 사용되고, 검증 후 오픈되지 않은 키복구 블럭만을 키관리 서버에 전송하므로 합법적 접근권을 보장한다.

그러나, 종래 기술인 베리사인사와 인트러스트사의 모델은 각각 키관리 서버와 인증 서버가 사용자의 암호용 개인키를 생성하므로, 키복구 과정이 아닌 키생성 과정에서 사용자의 암호용 개인키가 노출되는 위험이 있다. 또한, 종래 기술인 넷스케이프사의 모델의 경우에도 위탁되는 개인키와 공개키의 대응성을 검사하기 위해 데이터복구 관리자의 전송용 키로 사용자의 개인키가 암호화되어 전송되기 때문에 키복구 과정이 아닌 키위탁 과정에서 데이터 복구 관리자에게 개인키가 노출되게 된다.

또한, 실용성 및 완전 순방향 비밀성면에 있어서도 본 발명은 종래 기술에 비하여 우월한 특징적 요소를 갖추고 있다. 즉, 넷스케이프사와 인트러스트사 모델의 경우, 위탁된 사용자의 키는 그 키를 관리하는 서버의 관련키(넷스케이프사; 데이터 복구 관리자의 저장용 키, 인트러스트사; 인증 서버의 CAST-128 또

는 3-DES 키)로 암호화되어 데이터베이스에 저장되므로 그 키를 별도로 안전하게 관리하여야 하며, 이것이 일단 공개되면 데이터베이스에 저장된 사용자의 암호용 개인키는 노출되게 된다.

또한, 베리사인사의 모델의 경우에도 키복구 서버는 키복구 블럭으로부터 복호화한 3-DES 키를 키관리 서버에게 안전하게 전송하기 위해 CRS 프로토콜을 이용하여야 한다. 따라서, 키관리 서버는 CRS 프로토콜을 위한 키를 별도로 안전하게 관리하여야 하며, 이를 노출시켜서는 아니 된다. 여기서, CRS 프로토콜은 전송되는 메시지에 대한 암호화와 서명을 수행한다.

반면에, 본 발명은 블라인드 디코딩(blind decoding)을 수행하여 키관리 서버가 별도의 암호용 공개키와 개인키를 관리할 필요가 없도록 함으로써 완전 순방향 비밀성 기능을 제공할 수 있다. 본 발명에 따른 키위탁 시스템의 경우, 사용자의 암호용 키는 사용자 자신만이 아는 패스워드로 암호화되어 있으므로, 사용자의 패스워드 확인자 만을 가지고 있는 키관리 서버는 키생성 과정 및 복구 과정에서 사용자의 암호용 개인키를 알아낼 수 없다. 또한, 블라인드 디코딩 기법을 사용하여 암호키 복구 과정에서 어떠한 키복구 서버도 사용자 키와 관련된 정보를 알아낼 수 없다.

또한, 본 발명에 따른 키위탁 시스템은 키복구 저장 장소의 장애 허용성을 보장한다. 즉, 종래 기술에 따른 넷스케이프사, 베리사인사 및 인트러스트사의 모델의 경우, 주기적으로 데이터베이스를 백업함으로써 장애 허용성을 보장하는 것으로 인식될 수도 있으나, 하나의 데이터베이스에 저장됨으로써 해킹 공격 목표가 집중될 수 있다.

반면에, 본원 발명에 따른 키위탁 시스템에서 키관리 서버는 사용자의 키복구 정보를 비밀 분산 알고리즘을 사용하여 여러 개의 데이터베이스에 분산해 저장하므로, 데이터베이스의 장애 허용 기능을 제공하고 공격 목표를 분산한다. 본 발명에 따른 양호한 실시예로서, 프로액티브 씨큐어(proactive secure) 비밀 분산 알고리즘을 적용하여 안전성을 향상시킬 수 있다.

프로액티브 씨큐어 비밀 분산 알고리즘은 알.오스트로브스키 및 엠.영 저술의 'How to withstand mobile virus attacks'(1991년도 제10차 ACM 심포지움 프로시딩 제51쪽 내지 제61쪽)에 상술되어 있다.

또한, 본 발명은 종래 기술인 클리퍼와 달리 소프트웨어나 하드웨어 형태로 구현이 가능하므로 구현 형태에 대한 유연성을 제공한다. 종래 기술로서 클리퍼에 관한 기술은 1994년 미국 표준 연구소(NIST)에 의해 발간된 FIBS PUB(Federal Information Processing Standards Publication)의 'Escrow Encryption Standard (EES)'를 참조할 수 있다.

본 발명에 따른 키위탁 시스템은 복구된 $C = E_{PWD}(PRI)$를 '패스워드 기반 다운로드 프로토콜'을 이용하여 안전하게 사용자에게 전송하도록 설계하였으므로, PKI-로밍 서비스가 가능하도록 확장할 수 있는 특징을 구비한다. 본 발명에 따른 강제적 키위탁 시스템은 종래 기술과는 달리 암호키 복구 권한을 분산함으로써 키복구에 대한 키복구 서버의 권한 남용을 방지할 수 있다.

이 때에, 본 발명에 따른 양호한 실시예로서 본원 발명의 출원인이 선출원한 대한민국 특허출원 제10-2000-0071859호에 개시되어 있는 'RSA 공개키 암호 고속화 방법'을 사용함으로써 암호키 복구 과정을 고속화할 수 있다. 또한, 본 발명에 따른 강제적 키위탁 시스템의 제2 실시예의 경우에 키관리 서버는 사전 공격을 통해 사용자의 암호용 개인키를 알아낼 수 있으므로, 대량 감청을 방지할 수 있다.

일반적으로, 송신자와 수신자는 디피-헬만(Diffie-Hellman)의 키 교환 방식을 이용해서 자신들의 세션키를 협약한다. 그러나, 이 때 사용자의 긴 주기의 개인키가 일단 공개되면 그 사용자의 이후와 이전의 모든 통신은 노출되게 된다. 따라서, 키복구에서 문제가 되는 것은 감청 기한의 제한 문제이다.

따라서, 본 발명의 양호한 실시예로서, 에이.케이.렌스트라 등이 제안한 세션키 분배 방식을 적용함으로써, 특정 기간 동안만 사용자에 대한 감청을 수행하도록 하는 방식이 적용될 수 있다. 참고로, 세션키 분배 기술에 대한 자료는 1995년 스프링거 베래그(Springer-Verlag) 출판사가 발간한 서적 'Advances in Cryptology -Crypto 95'의 제197쪽 내지 제207쪽에 실려있는 문헌 'A key escrow system with warrant bounds'에 개시되어 있다.

이하에서는, 본 발명의 또 다른 양호한 실시예로서 디피 헬만 기반의 키위탁 시스템 기술을 상술한다. 이하에서 사용되는 기호를 먼저 설명하면 다음과 같다. 본 발명에서 PWD는 PKI-로밍 서비스를 위한 사용자 A의 패스워드를 의미한다.

또한, VER은 PKI-로밍 서비스를 위하여 키관리 서버에 등록된 사용자 A의 패스워드 확인자이다. 한편, KRB는 사용자 A에 대한 키복구 블럭을 나타내고, P는 소수로서 P = qw + 1을 만족하고, q는 큰 소수이며 w는 유연한(smooth) 합성수를 나타낸다. 또한, g는 그룹의 원시원소이고 g의 차수는 order(g) = q를 만족한다. 이하, 발명의 상세한 설명에서 (x_i, y_i)는 제i번째 키복구 서버(KRA_i)의 암호용 비밀키/공개키 쌍을 나타내며, $y_i = g^{x_i} \bmod p$의 관계가 성립한다.

도7a는 본 발명에 따른 키위탁 시스템의 제4 실시예를 나타낸 것으로서, 디피-헬만 기반의 (n,n)-상업용 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 도7a를 참조하면, 사용자 A(10)는 자신의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고, KRB를 아래와 같이 생성하여 PUB과 함께 등록 서버(RA; 11)에 전송한다(단계 S410).

먼저, 사용자 A(10)는 PRI를 자신의 PWD로 암호화한다. 즉, $C = E_{PWD}(PRI)$를 계산한다. 이어서, 난수 z를 0 < z < q의 범위에서 선택한다. 또한, KRB를 아래의 수학식 7을 이용하여 생성한다.

$$KRB = (C_1, C_2) = (g^z \bmod p, C \cdot (y_1 \cdot y_2 \cdot \cdots \cdot y_n)^z \bmod p)$$

한편, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 KRB와 PUB을 전송한다 (단계 S411). 또한, 키관

리 서버(KMA; 13)는 (m, ℓ)-비밀 분산 알고리즘(단, m < ℓ)을 사용하여 KRB를 ℓ개로 조각낸 후, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스(DB_1(21), DB_2(22), …DB_ℓ(23))에 각각 나누어 저장한다. 저장을 마친 후 KRB는 소거한다.

이어서, 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 '암호용 인증서 발급 허가서'를 전송한다(단계 S412). 본 발명에 따른 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)의 '암호용 인증서 발급 허가서'를 제시한 후, 사용자 A(10)의 암호용 공개키 PUB에 대한 암호용 인증서를 요청한다(단계 S413). 그 결과, 인증 서버(CA; 12)는 암호용 인증서를 발급한 후, 디렉토리 서버 (19)에 사용자 A(10)의 암호용 인증서를 공개하고 등록 서버(RA; 11)에게 암호용 인증서를 전송한다(단계 S414). 마지막으로, 등록 서버(RA; 11)는 암호용 인증서를 사용자 A(10)에게 전송한다(단계 S415).

도7b는 본 발명에 따른 키위탁 시스템의 양호한 실시예를 나타내는 것으로서, 디피-헬만 기반의 (n,n)-상업적 키위탁 시스템의 키복구 과정을 나타낸 도면이다. 도7b를 참조하면, 사용자 A(10)는 키관리 서버(KMA; 13)에게 자신의 암호용 개인키의 복구를 요청한다(단계 S550). 본 발명에 따른 키관리 서버(KMA; 13)는 사용자 A(10)를 확인한 후, 데이터베이스(21, 22, 23) 검색을 통하여 사용자 A(10)에 대한 ℓ개의 키복구 블럭 조각 중 m개의 키복구 블럭 조각 KRB_1, KRB_2, …, KRB_m을 취합하고, (m, ℓ)-비밀 분산 알고리즘(단, m < ℓ)을 이용하여 KRB를 재구성한다.

한편, 키관리 서버(KMA; 13)는 다음 과정을 통하여 사용자 A(10)의 $E_{PWD}(PRI)$를 복구한다. 우선, 키관리 서버(KMA; 13)는 은닉 인자(blind factor) r(0 < r < P-1)을 랜덤하게 선택한 후, C_1'를 계산하여 '암호용 개인키 복구 요청서'와 함께 키복구 서버(KRA_1, KRA_2, …, KRA_n)에게 각각 전송한다.

여기서, C_1'은 $C_1' \equiv C_1^r \bmod P$의 관계가 성립한다. 또한, 각각의 KRA_i는 $C_1''_{(i)} \equiv (C_1')^{x_{(i)}} \bmod P$를 계산하여 키관리 서버(KMA; 13)에게 전송한다(단, i = 1, …, n). 이어서, 키관리 서버(KMA; 13)는 $C_2 / (C_1''_{(1)} \cdot C_1''_{(2)} \cdot \cdots \cdot C_1''_{(m)})^r \bmod P$를 계산하여 $E_{PWD}(PRI)$를 복구한다.

한편, 사용자 A(10)의 패스워드 확인자를 소지한 키관리 서버(KMA; 13)는 복구된 사용자 A(10)의 $E_{PWD}(PRI)$를 '패스워드 기반 다운로드 프로토콜'을 이용하여 안전하게 사용자 A(10)에게 전송한다.

도8은 본 발명에 따른 키위탁 시스템의 제5 실시예를 나타낸 것으로서, 디피-헬만 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 본 발명에 따른 제5 실시예는 본 발명의 제4 실시예를 대량 감청 방지 기능을 구비한 강제적 키위탁 시스템으로 활용하고자 하는 경우, 등록 서버가 위탁되는 사용자의 키복구 블럭에 대하여 정당성을 검증하는 과정을 구비하고 있음을 특징으로 한다.

도8을 참조하면, 본 발명의 제5 실시예에 따라 사용자 A(10)는 s개의 패스워드 PWD_j(단, j = 1, …, s)를 생성한 후, 이에 대응하는 s개의 패스워드 확인자 VER_j(단, j = 1, …, s)를 키관리 서버(KMA; 13)에 등록한다(단계 S510). 또한, 사용자 A(10)는 s개의 암호용 개인키/공개키 쌍(PRI_j, PUB_j)을 생성한다. 이어서, 사용자 A(10)는 s개의 KRB_j(단, j = 1, …, s)을 아래와 같이 생성하여 PUB_j(단, j = 1, …, s)와 함께 등록 서버 (RA; 11)에 전송한다(단계 S511).

우선, 사용자 A(10)는 개인키 PRI_j를 자신의 패스워드 PWD_j로 암호화한다. 즉, $C_j \equiv E_{PWD_j}(PRI_j)$(단, j = 1, …, s)를 계산한다. 이 때에, 본 발명의 바람직한 실시예로서, 긴급 감청 기능이 필요한 키위탁 시스템으로 활용하고자 하는 경우에는 사용자가 KRB를 생성하는 단계에서 패스워드 PWD를 이용한 암호화 과정을 수행하지 않을 수 있다.

이어서, s개의 난수 $0 < z_j < q$ (단, j = 1, …, s)를 선택하고, KRB_j(단, j = 1, …, s)를 아래 수학식 8을 이용하여 산출한다.

$$KRB_j \equiv (C_{z_j}, C_{z_j}) \equiv (g^{z_j} \bmod P, C_j \cdot (x_1 \cdot x_2 \cdot \cdots \cdot x_m)^{z_j} \bmod P)$$

한편, 등록 서버(RA; 11)는 $1 \le k \le s$ 범위에서 난수 k를 선택하여 사용자에게 전송한다(단계 S512). 이 때에, 본 발명의 바람직한 실시예로서 s의 크기를 변화시킴으로써 보안 강도의 조절을 가능하도록 할 수 있다.

다시 도8을 참조하면, 사용자 A(10)는 KRB_k를 제외한 (s-1)개의 나머지 KRB_j를 오픈(open)한다(단계 S513). 즉, PWD_j, PRI_j, z_j(단, $\forall j \neq k$, $1 \le j \le s$)를 등록 서버(RA; 11)에게 전송한다. 한편, 등록 서버 (RA; 11)는 사용자 A(10)로부터 받은 정보를 이용하여 PRI_j와 PUB_j의 대응성 및 KRB_j의 정당성을 검사한다. 본 발명의 또 다른 실시예로서, 개인키와 공개키의 대응성 및 키복구 블럭의 정당성을 검사하는 과정은 해쉬 함수를 이용하여 비대화형 방식으로 설계할 수도 있다.

이어서, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 $KRB = KRB_k$와 $PUB = PUB_k$를 전송한다(단계 S514). 이하, 단계 S515 내지 단계 S518은 본 발명의 제4 실시예의 과정과 동일하다. 한편, 보다 실용적이고 강력한(섀도우 공개키 공격에 대해서도 안전한) 디피-헬만 기반의 (n,n)-강제적 키위탁 시스템을 구현하고자 하는 경우, 본 발명의 제6 실시예로서, 키관리 서버가 사용자의 개인키/공개키 쌍을 생성한 후 패스워드로 암호화하여 사용자에게 전송하는 방식을 사용할 수 있다.

도9는 본 발명의 제6 실시예를 나타낸 것으로서, 디피-헬만 기반의 (n,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 사용자 A(10)는 등록 서버(RA; 11)에게 암호용 인증서 발급을 요청한다(단계 S630). 등록 서버 (RA; 11)는 키관리 서버(KMA; 13)에게 이를 다시 전송한다(단계 S631). 한편, 키관리 서버(KMA; 13)는 사용자 A(10)의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고, 키복구 블럭(KRB)을 아래와 같이 생성하여 데이터베이스(21, 22, 23)에 분산 저장한다(단계 S632).

우선, 키관리 서버는 사용자의 PRI를 PWD로 암호화한다. 즉, $C = E_{PWD}(PRI)$을 계산한다. 이 때에, 키관리 서버(KMA; 13)에는 사용자 A(10)의 PWD가 사전에 등록되어 있다고 가정한다. 이어서, 난수 z를 $0 < z < q$의 범위에서 선택한다. 또한, KRB를 아래의 수학식 9를 이용하여 생성한다.

$$KRB = (C_1, C_2) = (g^z \bmod P,\ C \cdot (y_1 \cdot y_2 \cdot \cdots \cdot y_n)^z \bmod P)$$

이어서, 본 발명에 따른 키관리 서버(KMA; 13)는 (m, ℓ)-비밀 분산 알고리즘(단, $m < \ell$)을 사용하여 KRB를 ℓ개로 조각낸 후, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스 (DB_1, DB_2, …, DB_ℓ)에 각각 나누어 저장한다. 저장을 마친 후 KRB를 소거한다.

또한, 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 '암호용 인증서 발급 허가서 및 (C, PUB)을 전송한다(단계 S633). 이어서, 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)로부터 전송된 '암호용 인증서 발급 허가서'를 제시한 후, 사용자 A(10)의 PUB에 대한 암호용 인증서를 요청한다(단계 S634).

또한, 본 발명에 따른 인증 서버(CA; 12)는 암호용 인증서를 발급한 후, 디렉토리 서버에 사용자 A(10)의 암호용 인증서를 공개하고(단계 S635) 등록 서버 (RA; 11)에게 암호용 인증서를 전송한다(단계 S636). 이어서, 등록 서버(RA; 11)는 암호용 인증서 및 C를 사용자 A(10)에게 전송한다(단계 S637).

본 발명의 제5 실시예에 따른 강제적 키위탁 시스템의 경우에는, 도7b에 나타낸 키복구 방식을 사용하여 위탁키를 복구할 수 있으며, 이 경우에는 키관리 서버가 사용자 패스워드에 대한 사전 공격을 통해 사용자의 암호용 개인키 PRI를 복구할 수 있다.

본 발명의 제6 실시예에 따른 강제적 키위탁 시스템의 경우에는 도7b를 나타낸 키복구 방식을 사용하여 위탁키를 복구할 수 있으며, 이 경우에는 키관리 서버는 자신이 가지고 있던 사용자의 패스워드를 이용하여 사용자의 암호용 개인키를 복구할 수 있다.

이하에서는, 본 발명에 따른 키위탁 시스템의 또 다른 바람직한 실시예로서, 디피-헬만 기반의 (t,n)-키위탁 시스템 기술을 상술한다. 단, $t < n$이다. 본 발명에 따른 디피-헬만 기반의 (t,n)-키위탁 시스템은 n개의 키복구 서버 중 t개만이 키복구에 참여해도 키복구가 가능함을 특징으로 한다.

이하에서 사용되는 용어를 먼저 설명하면 다음과 같다. 본 발명에서 PWD는 PKI-로밍 서비스를 위한 사용자의 패스워드를 의미한다. 또한, VER은 PKI-로밍 서비스를 위하여 키관리 서버에 등록된 사용자의 패스워드 확인자를 나타낸다.

또한, KRB는 사용자 A에 대한 키복구 블럭을 의미하고, P는 소수로서, $P = qw + 1$을 만족하고, q는 큰 소수이며 w는 유연한 합성수이다. 또한, g는 그룹의 원시원소이고, $order(g) = q$를 만족한다. 또한, x_i는 제i번째 키복구 서버 KRA_i의 개인키로서 $1 \le i \le n$이다.

이하에서, y는 키복구 서버들의 그룹 공개키로서 아래와 같이 생성된다. 즉, 각각의 KRA_i(단, $1 \le i \le n$)는 난수 $r_i \in_R Z_q$를 선택한 후, $y_i = g^{r_i} \bmod P$를 계산하여 공개한다. 이어서, 각각의 KRA_i는 $f_i(0) = r_i$인 t-1차의 다항식 f_i를 Z_q 상에서 랜덤하게 선택한다. 즉, $f_i(x) = r_i + a_{i,1} \cdot x + a_{i,2} \cdot x^2 + \cdots + a_{i,t-1} \cdot x^{t-1} \bmod q$(단, $a_{i,1}, a_{i,2}, \cdots, a_{i,t-1} \in_R Z_q$)을 랜덤하게 선택한다.

KRA_i는 $f_i(j) \bmod q$ (단, $\forall j \neq i$, $1 \le j \le n$)을 계산하여 KRA_j에게 비밀리에 전송한다. 또한, $g^{a_{i,1}} \bmod P, g^{a_{i,2}} \bmod P, \cdots, g^{a_{i,t-1}} \bmod P$를 계산하여 공개한다. 또한, 각각의 KRA_i는 전송받은 $f_j(i)$(단, $\forall j \neq i$, $1 \le j \le n$)를 이용하여 다음 식으로 그 정당성을 검증할 수 있다.

$$g^{f_j(i)} \stackrel{?}{=} y_j \cdot (g^{a_{j,1}})^{i} \cdot \cdots \cdot (g^{a_{j,t-1}})^{i^{t-1}} \bmod P$$ (단, $\forall j \neq i$, $1 \le j \le n$)

한편, $H \stackrel{def}{=} \{KRA_i \mid$ KRA_i는 전술한 단계를 통과한 모든 정직한 키복구 서버$\}$이라 하면, 이제 각 KRA_i는 자신의 개인키 $x_i = \sum_{j \in H} f_j(i)$를 계산하여 비밀리에 보관한다. 키복구 서버들은 자신들의 그룹 공개키 y를 다음과 같이 계산하여 공개할 수 있다. 즉, 본 발명의 양호한 실시예로서, $y = \prod_{j \in H} y_j$의 식을 사용할 수 있다.

앞에서 전술한 것과 같이 패터슨이 1991년 스프링거 배래그 출판사가 발견한 'Advances in Cryptology-Eurocrypt '91'의 제522쪽 내지 제526쪽에 실려있는 문헌 'A threshold cryptosystem without a trusted party'에 개시된 방식으로 생성되는 그룹 공개키는 균일하게 분포되지 않는다는 문제점이 Gennaro, Janecki, Krawczyk, Rabin에 의해 지적되었으나, 본 발명에서는 실용적인 측면을 우선적으로 고려하므로 패터슨 스킴을 이용하였다.

도10은 본 발명에 따른 키위탁 시스템의 제7 실시예를 나타낸 것으로서, 디피-헬만 기반의 (t,n)-상업용

키위탁 시스템의 키생성 및 키위탁 과정과 키복구 과정을 각각 도10a와 도10b에 나타내고 있다. 이하에서는, 도10a 및 도10b를 참조하여 본 발명의 제7 실시예에 따라 키위탁 과정과 생성·위탁된 키를 복구하는 방법을 상세히 설명한다.

도10a를 참조하면, 사용자 A(10)는 자신의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고, 키복구 블럭(KRB)을 아래와 같이 생성하여 공개키 PUB과 함께 등록 서버(RA; 11)에 전송한다(단계 S710).

먼저, 사용자 A(10)는 PRI를 자신의 PWD로 암호화한다. 즉, $C = E_{PWD}(PRI)$를 계산한다. 이어서, 난수 z를 $0 < z < q$의 범위에서 선택한다. 또한, 키복구 블럭(KRB)을 아래의 수학식 10을 이용하여 생성한다.

$$KRB = (C_1, C_2) = (g^z \bmod P, C \cdot y^z \bmod P)$$

한편, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 KRB와 PUB을 전송한다 (단계 S711). 또한, 키관리 서버(KMA; 13)는 (m, ℓ)-비밀 분산 알고리즘(단, $m < \ell$)을 사용하여 KRB를 ℓ개로 조각낸 후, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스(DB_1(21), DB_2(22), …DB_ℓ(23))에 각각 나누어 저장한다. 저장을 마친 후 KRB를 소거한다.

이어서, 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 '암호용 인증서 발급 허가서'를 전송한다(단계 S712). 본 발명에 따른 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)로부터 전송받은 '암호용 인증서 발급 허가서'를 제시한 후, 사용자 A(10)의 암호용 공개키 PUB에 대한 암호용 인증서를 요청한다(단계 S713). 그 결과, 인증 서버(CA; 12)는 암호용 인증서를 발급한 후, 디렉토리 서버(19)에 사용자 A(10)의 암호용 인증서를 공개하고 등록 서버(RA; 11)에게 암호용 인증서를 전송한다(단계 S714). 마지막으로, 등록 서버(RA; 11)는 암호용 인증서를 사용자 A(10)에게 전송한다(단계 S715).

도10b를 참조하여 본 발명의 제7 실시예에 따라 위탁된 키를 복구하는 방법을 설명하면 아래와 같다. 우선, 사용자 A(10)가 키관리 서버(KMA; 13)에 자신의 암호용 개인키의 복구를 요청하게 되면(단계 S850), 키관리 서버(KMA; 13)는 사용자 A(10)를 확인한 후, 데이터베이스 검색을 통하여 사용자 A(10)에 대한 ℓ개의 키복구 블럭 조각 중 m개의 키복구 블럭 조각 KRB_1, KRB_2, …, KRB_m을 취합하고, (m, ℓ)-비밀 분산 알고리즘(단, $m < \ell$)을 이용하여 KRB를 재구성한다.

이어서, n개의 키복구 서버 중에서 t개 이상만 동의한다면, 키관리 서버 (KMA; 13)는 다음의 과정을 통하여 사용자 A(10)의 $E_{PWD}(PRI)$를 복구할 수 있다. 우선, 키관리 서버(KMA; 13)는 은닉 인자 $r(0 < r < P-1)$을 랜덤하게 선택한 후, C_1'를 계산하여 '암호용 개인키 복구 요청서'와 함께 KRA_1, KRA_2, …, KRA_n에게 각각 전송한다. 즉, $C_1' = C_1 r^e \bmod P$ 의 관계식이 성립한다.

그리고, t개의 키복구 서버 KRA_i는 각각 $C_1''_{(i)} = (C_1')^{x_i} \bmod P$를 계산하여 $(C_1''_{(i)}, i)$를 키관리 서버(KMA; 13)에게 전송한다. 또한, 키관리 서버(KMA; 13)는 t개의 키복구 서버로부터 t개의 $(C_1''_{(i)}, i)$ 쌍을 수신한 후, 이로부터

$$C = C_2 / \prod_i (C_1''_{(i)})^{r \cdot \lambda_{i(0)}} \bmod P$$

를 계산하여 $C = E_{PWD}(PRI)$를 복구한다.

마지막으로, 사용자 A(10)의 패스워드 확인자를 소지한 키관리 서버(KMA; 13)는 복구된 사용자 A(10)의 $C = E_{PWD}(PRI)$를 '패스워드 기반 다운로드 프로토콜'을 이용하여 안전하게 사용자 A(10)에게 전송한다.

본 발명에 따른 디피-헬만 기반의 (t,n)-상업용 키위탁 시스템을 대량 감청 방지 기능을 갖는 강제적 키위탁 시스템으로 활용하고자 하는 경우, 등록 서버가 위탁되는 사용자의 키복구 블럭에 대해 정당성을 검증하는 과정이 필요하며, 전술한 제2 실시예에서와 같이 컷앤쵸즈 기법을 사용할 수 있다.

이어서 설명하는 본 발명의 제8 실시예는 컷앤쵸즈 기법이 적용된 디피-헬만 기반의 (t,n)-강제적 키위탁 시스템을 개시한다.

도11은 본 발명의 제8 실시예를 나타낸 것으로, 디피-헬만 기반의 (t,n)-강제적 키위탁 시스템의 키생성 및 키위탁 과정을 나타낸 도면이다. 도11의 구성을 살펴 보면, 도8에 나타낸 제5 실시예의 시스템 구성과 동일하게 보이지만 키복구 블럭(KRB)의 구성 부분이 서로 상이함을 인식하여야 한다(도면 상에는 도시되지 않음).

도11을 참조하면, 본 발명의 제8 실시예에 따라 사용자 A(10)는 s개의 패스워드 PWD_j(단, $j = 1, \cdots, s$)를 생성한 후, 이에 대응하는 s개의 패스워드 확인자 VER_j(단, $j = 1, \cdots, s$)를 키관리 서버(KMA; 13)에 등록한다(단계 S910). 또한, 사용자 A(10)는 s개의 암호용 개인키/공개키 쌍(PRI_j, PUB_j)을 생성한다. 이어서, 사용자 A(10)는 s개의 KRB_j(단, $j = 1, \cdots, s$)을 아래와 같이 생성하여 PUB_j(단, $j = 1, \cdots, s$)와 함께 등록 서버 (RA; 11)에 전송한다(단계 S911).

우선, 사용자 A(10)는 개인키 PRI_j를 자신의 패스워드 PWD_j로 암호화한다. 즉, $C_j = E_{PWD_j}(PRI_j)$(단, $j = 1, \cdots, s$)를 계산한다. 이 때에, 본 발명의 바람직한 실시예로서, 긴급 감청 기능이 필요한 키위탁

시스템으로 활용하고자 하는 경우에는 사용자가 키복구 블럭을 생성하는 단계에서 패스워드를 이용한 암호화 과정을 수행하지 않을 수 있다.

이어서, s개의 난수 $0 < z_j < q$ (단, $j = 1, \cdots, s$)를 선택하고, KRB_j(단, $j = 1, \cdots, s$)를 아래 수학식 11을 이용하여 산출한다.

$$KRB_j = (C_1, C_2) = (g^z \bmod p, \cdot \cdot y^z \bmod p)$$

한편, 등록 서버(RA; 11)는 난수 k를 $1 \leq k \leq s$의 범위에서 선택하여 사용자에게 k를 전송한다(단계 S912). 이 때에, 본 발명의 바람직한 실시예로서 s의 크기를 변화시킴으로써 보안 강도의 조절을 가능하도록 할 수 있다.

다시 도11을 참조하면, 사용자 A(10)는 KRB_k를 제외한 (s-1)개의 나머지 KRB_j를 오픈한다(단계 S913). 즉, PWD_j, PRI_j, z_j(단, $\forall j \neq k$, $1 \leq j \leq s$)를 등록 서버(RA; 11)에게 전송한다. 한편, 등록 서버(RA; 11)는 사용자 A(10)로부터 받은 정보를 이용하여 PRI_j와 PUB_j의 대응성 및 KRB_j의 정당성이 검증되면 j = k인 경우에 대해서도 대응성 및 정당성이 검증된 것으로 간주한다. 본 발명의 또 다른 실시예로서, 개인키와 공개키의 대응성 및 키복구 블럭의 정당성을 검사하는 과정은 해쉬 함수를 이용하여 비대화형 방식으로 설계할 수도 있다.

이어서, 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 $KRB = KRB_k$와 $PUB = PUB_k$를 전송한다(단계 S914). 이하, 단계 S915 내지 단계 S919는 본 발명의 제4 실시예의 과정과 동일하다.

또 다른 양호한 실시예로서, 본 발명에 따른 디피-헬만 기반의 (t,n)-상업용 키위탁 시스템을 보다 실용적이며 강력한(Shadow 공개키 공격에도 안전한) 강제적 키위탁 시스템을 설계하고자 할 경우, 키관리 서버가 사용자의 개인키/공개키 쌍을 생성한 후, 패스워드로 암호화하여 사용자에게 전송하도록 할 수 있다.

즉, 도12는 본 발명의 제9 실시예를 나타낸 것으로, 디피-헬만 기반의 (t,n)-강제적 키위탁 시스템의 키 생성 및 키위탁 과정을 나타낸 도면이다.

도12의 구성을 살펴 보면, 도9에 나타낸 제6 실시예의 시스템 구성과 동일하게 보이지만 키복구 블럭(KRB)의 구성 부분이 서로 상이함을 인식하여야 한다(도면 상에는 도시 되지 않음).

사용자 A(10)은 등록 서버(RA; 11)에게 암호용 인증서 발급을 요청한다(단계 S1210). 등록 서버(RA; 11)는 키관리 서버(KMA; 13)에게 이를 다시 전송한다(단계 S1211). 한편, 키관리 서버(KMA; 13)는 사용자 A(10)의 암호용 개인키/공개키 쌍(PRI, PUB)을 생성하고 키복구 블럭(KRB)을 아래와 같이 생성하여 데이터베이스 (DB_1(21), DB_2(22), …, DB_ℓ(23))에 분산 저장한다.

우선, 키관리 서버(KMA; 13)는 사용자 A(10)의 PRI를 사용자 A(10)의 패스워드(PWD)로 암호화 한다. 즉, $C = E_{PWD}(PRI)$를 계산한다. 이 때에 키관리 서버(KMA; 13)에는 사용자 A(10)의 PWD가 사전에 등록되어 있다고 가정한다. 이어서, 키관리 서버(KMA; 13)는 $0 < z < q$의 범위에서 난수 z를 선택하여 KRB를 산출한다. 즉, KRB는 $KRB = (C_1, C_2) = (g^z \bmod p, C \cdot y^z \bmod p)$의 계산식으로부터 산출된다.

이어서, 본 발명에 따른 키관리 서버(KMA; 13)는 (m, ℓ)-비밀 분산 알고리즘(단, $m < \ell$)을 사용하여 KRB를 ℓ개로 조각낸 후, 각각의 조각 KRB_1, KRB_2, …, KRB_ℓ을 사용자의 개인 식별 정보와 함께 ℓ개의 데이터베이스 (DB_1, DB_2, …, DB_ℓ)에 각각 나누어 저장한다. 저장을 마친 후 KRB를 소거한다.

또한, 키관리 서버(KMA; 13)는 등록 서버(RA; 11)에게 '암호용 인증서 발급 허가서 및 (C, PUB)을 전송한다(단계 S1212). 이어서, 등록 서버(RA; 11)는 인증 서버(CA; 12)에게 키관리 서버(KMA; 13)의 '암호용 인증서 발급 허가서'를 제시한 후, 사용자 A(10)의 PUB에 대한 암호용 인증서를 요청한다(단계 S1213).

또한, 본 발명에 따른 인증 서버(CA; 12)는 암호용 인증서를 발급한 후, 디렉토리 서버에 사용자 A(10)의 암호용 인증서를 공개하고 등록 서버(RA; 11)에게 암호용 인증서를 전송한다(단계 S1214). 이어서, 등록 서버(RA; 11)는 암호용 인증서 및 C를 사용자 A(10)에게 전송한다(단계 S1215).

본 발명의 제8 실시예에 따른 강제적 키위탁 시스템의 경우에는 도10b에 나타낸 키복구 방식을 이용하여 사용자의 개인키 PRI를 복구할 수 있으며, 이 때에 키관리 서버가 사용자 패스워드에 대한 사전 공격을 통해 사용자의 암호용 개인키 PRI를 복구할 수 있다.

본 발명의 제9 실시예에 따른 강제적 키위탁 시스템의 경우에는 도10b에 나타낸 키복구 방식을 이용하여 사용자의 개인키 PRI를 복구할 수 있으며, 이 때에 키관리 서버는 자신이 가지고 있던 사용자의 패스워드를 이용하여 사용자의 암호용 개인키를 복구할 수 있다.

전술한 내용은 후술할 발명의 특허 청구 범위를 보다 잘 이해할 수 있도록 본 발명의 특징과 기술적 장점을 다소 폭넓게 개설하였다. 본 발명의 특허 청구 범위를 구성하는 부가적인 특징과 장점들이 이하에서 상술될 것이다. 개시된 본 발명의 개념과 특정 실시예는 본 발명과 유사 목적을 수행하기 위한 다른 구조의 설계나 수정의 기본으로서 즉시 사용될 수 있음이 당해 기술 분야의 숙련된 사람들에 의해 인식되어야 한다.

또한, 본 발명에서 개시된 발명 개념과 실시예가 본 발명의 동일 목적을 수행하기 위하여 다른 구조로 수정하거나 설계하기 위한 기초로서 당해 기술 분야의 숙련된 사람들에 의해 사용되어질 수 있을 것이다. 또한, 당해 기술 분야의 숙련된 사람에 의한 그와 같은 수정 또는 변경된 등가 구조는 특허 청구

범위에서 기술한 발명의 사상이나 범위를 벗어나지 않는 한도 내에서 다양한 변화, 치환 및 변경이 가능하다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명은 PKI와 상호 연동되면서도 사용자와 정부의 요구 사항을 함께 충족시키는 실용적인 키위탁 시스템을 제공한다. 본 발명에 따른 키위탁 시스템은 PKI-로밍 시스템에 활용될 수 있으며, 키관리 서버에 완전 순방향 비밀성 개념을 부여함으로써 안정성을 증대하는 효과가 있다.

또한, 본 발명에 따른 키위탁 시스템은 강제적 시스템으로 활용될 경우에도 사용자의 프라이버시를 최대한 보장하는 효과가 있다.

(57) 청구의 범위

청구항 1

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 생성한 후, 이에 대응되는 패스워드 확인자를 키관리 서버에 등록하는 단계;

(b) 상기 사용자가 자신의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 사용자가 상기 패스워드를 이용하여 상기 개인키를 암호화하는 단계(즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD; 패스워드, PRI; 개인키);

(d) 상기 사용자가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키복구 블럭과 상기 공개키가 키관리 서버에게 전송되는 단계; 및

(f) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 상기 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 2

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 생성한 후, 이에 대응되는 패스워드 확인자를 키관리 서버에 등록하는 단계;

(b) 상기 사용자가 자신의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 사용자가 패스워드를 이용하여 상기 개인키를 암호화하는 단계 (즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD; 패스워드, PRI; 개인키);

(d) 상기 사용자가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키복구 블럭의 정당성을 확인하는 단계;

(f) 정당성이 확인된 키복구 블럭과 개인키와의 대응성이 확인된 공개키가 키관리 서버에게 전송되는 단계; 및

(g) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 3

제2항에 있어서, 상기 키생성 및 위탁 방법은 단계 (c)를 생략하고 단계 (d)에서 사용자가 키복구 서버의 암호용 공개키를 이용하여 사용자의 공개키를 암호화함으로써 키복구 블럭을 생성하는 것을 특징으로 하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 4

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 키관리 서버에 등록하는 단계;

(b) 키관리 서버가 상기 사용자의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 키관리 서버가 상기 사용자의 등록된 패스워드를 이용하여 상기 사용자의 개인키를 암호화하는 단계(즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD; 패스워드, PRI; 개인키);

(d) 상기 키관리 서버가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 상기 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 5

(a) 키관리 서버가 키복구 요청 메시지를 수신한 후, 위탁된 복구 대상자의 키복구 블럭을 재구성하는 단계;

(b) 상기 키관리 서버가 복수의 키복구 서버 중 어떤 키복구 서버도 키복구 블럭을 볼 수 없도록 하기 위해 자신만이 알고 있는 은닉 인자를 이용하여 키복구 블럭을 은닉하는 단계;

(c) 상기 키관리 서버가 은닉된 키복구 블럭을 암호용 개인키 복구 요청서와 함께 복수의 키복구 서버들에게 전송하는 단계;

(d) 상기 복수의 키복구 서버들이 수신한 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 단계;

(e) 상기 키복구 서버들이 복호화된 메시지를 키관리 서버에게 전송하는 단계;

(f) 상기 키관리 서버가 키복구 서버들로부터 수신한 메시지와 자신만이 알고 있는 은닉 인자를 이용하여 암호화된 사용자의 개인키 C를 복구하는 단계

를 포함하는 키위탁 시스템의 키복구 방법.

청구항 6

제5항에 있어서, 상기 단계 (a)의 키복구 요청은 사용자의 요청 또는 법원으로부터의 요청을 포함하는 키위탁 시스템의 키복구 방법.

청구항 7

제5항에 있어서, 상기 단계 (a)의 키복구 블럭 재구성 단계는 복수의 키복구 블럭 조각 중 일부만으로 키복구 블럭을 재구성하는 것을 포함하는 키위탁 시스템의 키복구 방법.

청구항 8

제5항에 있어서, 상기 단계 (f)의 암호화된 사용자의 개인키 복구 단계는 상기 키관리 서버가 복수의 키복구 서버 중 일부 키복구 서버로부터의 메시지만으로도 상기 암호화된 사용자의 개인키 C를 복구하는 것을 포함하는 키위탁 시스템의 키복구 방법.

청구항 9

제5항에 있어서, 키복구 요청자의 패스워드 확인자를 소지한 상기 키관리 서버가 복구한 암호화된 개인키 C를 패스워드 기반 다운로드 프로토콜을 이용하여 키복구 요청자에게 전송하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 10

제5항에 있어서, 키관리 서버 또는 신뢰 객체가 패스워드에 대한 사전 공격을 통해 C로부터 사용자의 암호용 개인키를 복구하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 11

제5항에 있어서, 키관리 서버 또는 신뢰 객체가 등록되어 있는 사용자의 패스워드를 이용하여 사용자의 암호용 개인키를 복구하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 12

PKI 기반의 키위탁 시스템의 서비스를 이용하고자, 패스워드를 생성한 후, 그에 대응되는 패스워드 확인자를 키관리 서버에 등록하고 자신의 암호용 개인키와 공개키 쌍을 생성한 후, 상기 패스워드를 이용하여 상기 개인키를 암호화한 $C = E_{PWD}(PRI)$ 단, PWD; 패스워드, PRI; 개인키)를 생성하고 키복구 서버들의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 사용자;

상기 키복구 블럭을 저장하거나 키복구 블럭을 여러 조각으로 분할한 키복구 블럭 조각을 분산 저장하며, 키복구 요청을 수신하는 경우, 상기 키복구 블럭을 재구성하고 복수의 키복구 서버 중 어떤 키복구 서버도 재구성된 키복구 블럭을 볼 수 없도록 하기 위해 자신만이 알고있는 은닉 인자를 이용하여 은닉한 키복구 블럭을 암호용 개인키 복구 요청서와 함께 상기 복수의 키복구 서버에게 전송하고, 상기 키복구 서버들로부터 수신한 메시지와 상기 은닉 인자를 이용하여 상기 C를 복구하는 키관리 서버; 및

암호용 개인키 복구 요청서와 함께 수신된 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 키복구 서버

를 포함하는 키위탁 시스템.

청구항 13

제12항에 있어서, 상기 사용자가 생성한 키복구 블럭의 정당성이 확인되는 것을 특징으로 하는 키위탁 시스템.

청구항 14

PKI 기반의 키위탁 시스템의 서비스를 이용하고자, 키관리 서버에 패스워드를 등록하는 사용자;

상기 사용자의 암호용 개인키와 공개키 쌍을 생성한 후, 상기 등록된 패스워드를 이용하여 상기 개인키를 암호화한 $C(=E_{PWD}(PRI))$ 단, PWD: 패스워드, PRI: 개인키)를 생성하고 키복구 서버들의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성한 후, 상기 키복구 블럭을 저장하거나 키복구 블럭을 여러 조각으로 분할한 키복구 블럭 조각을 분산 저장하며, 키복구 요청을 수신하는 경우, 상기 키복구 블럭을 재구성하고 복수의 키복구 서버 중 어떤 키복구 서버도 재구성된 키복구 블럭을 볼 수 없도록 하기 위해 자신만이 알고있는 은닉 인자를 이용하여 은닉한 키복구 블럭을 암호용 개인키 복구 요청서와 함께 상기 복수의 키복구 서버에게 전송하고, 상기 키복구 서버들로부터 수신한 메시지와 상기 은닉 인자를 이용하여 상기 C를 복구하는 키관리 서버; 및

암호용 개인키 복구 요청서와 함께 수신된 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 키복구 서버

를 포함하는 키위탁 시스템.

청구항 15

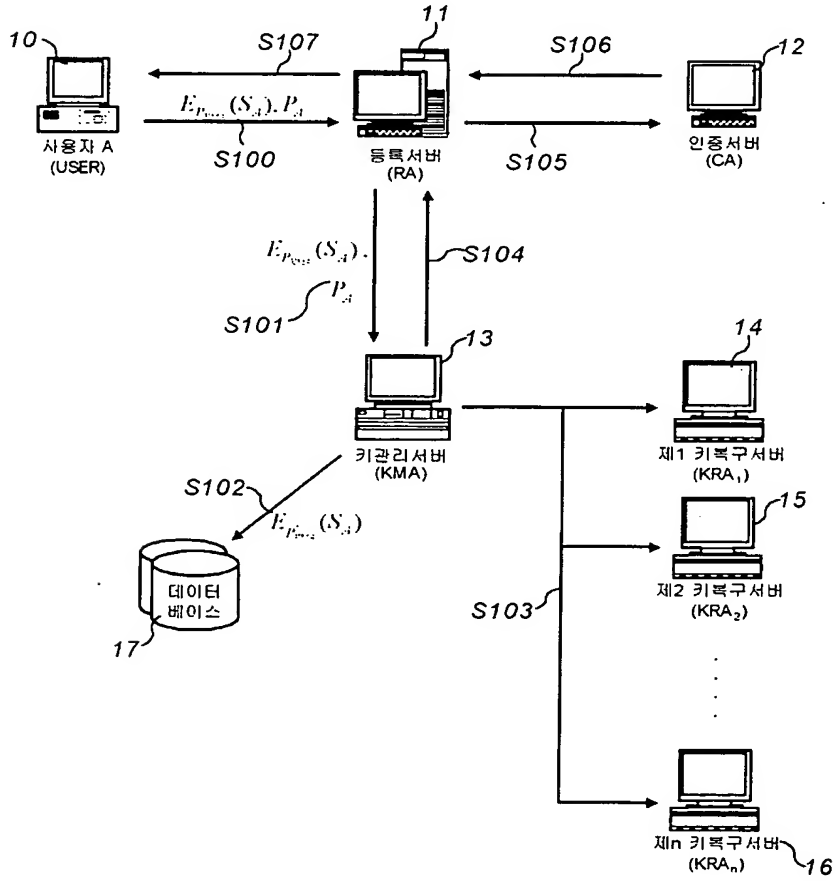
제12항 또는 제14항에 있어서, 복수의 키복구 블럭 조각 중 일부만으로도 키복구 블럭을 재구성하는 키관리 서버를 포함하는 키위탁 시스템.

청구항 16

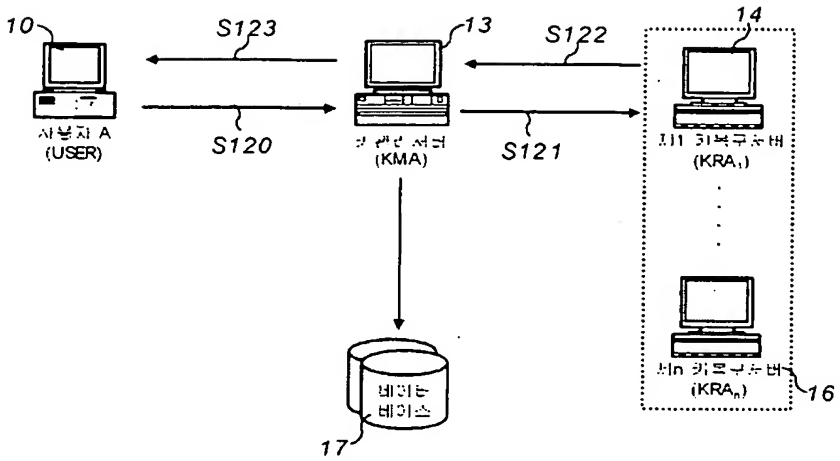
제12항 또는 제14항에 있어서, 복수의 키복구 서버 중 일부 키복구 서버로부터의 메시지만으로도 상기 암호화된 사용자의 개인키 C를 복구하는 키관리 서버를 포함하는 키위탁 시스템.

도면

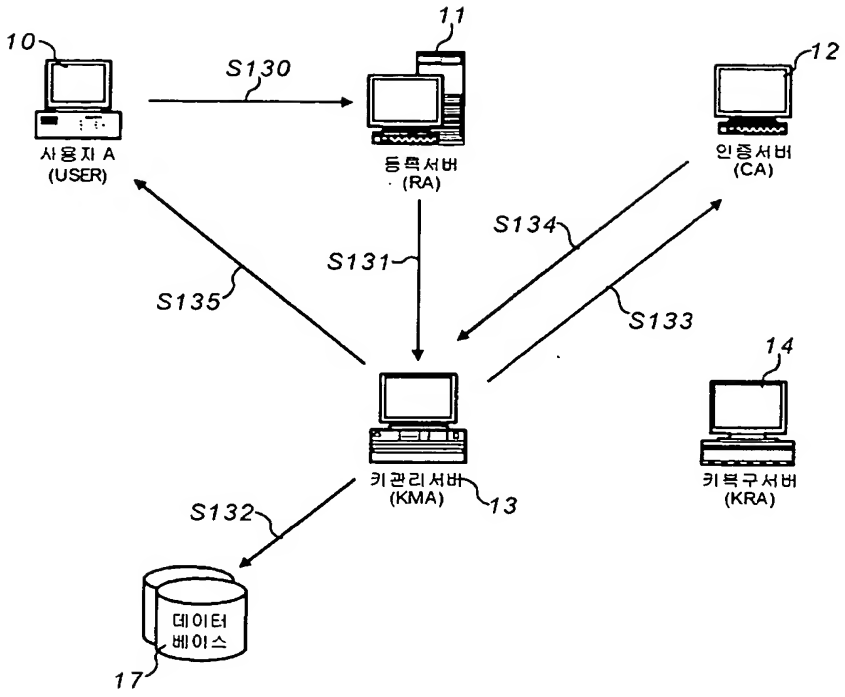
도면1a



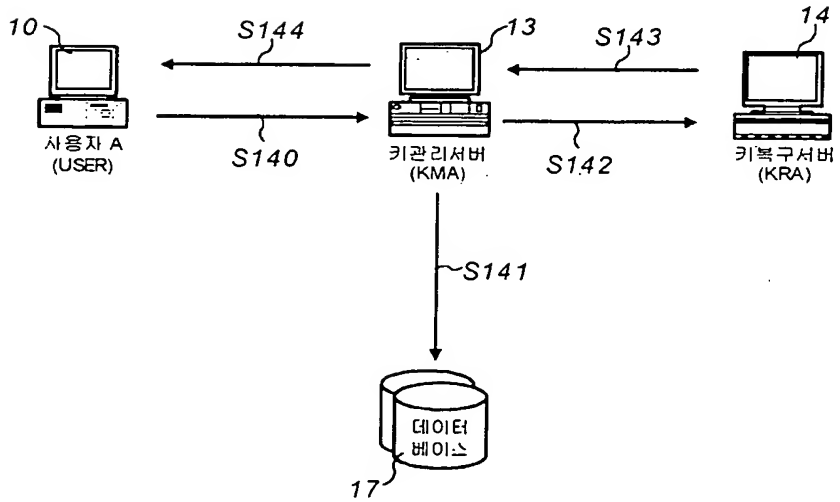
도면1b



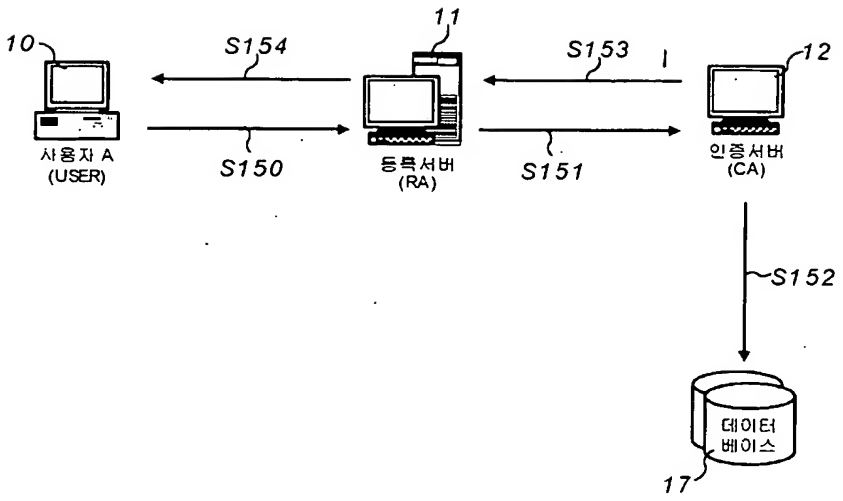
도면2a


10
11
12
S130
사용자 A
(USER)
등록서버
(RA)
인증서버
(CA)
S134
S131
S135
S133
14
키관리서버
(KMA)
13
키복구서버
(KRA)
S132
데이터
베이스
17

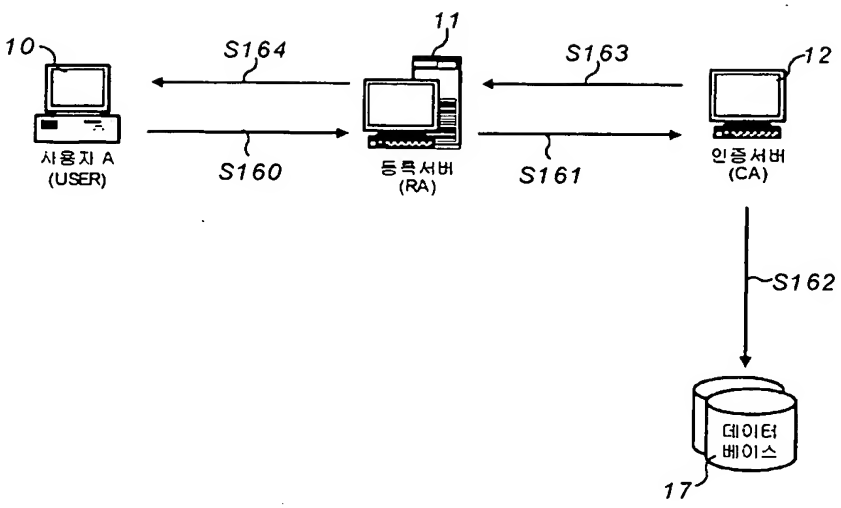
도면2b


10
S144
13
S143
14
사용자 A
(USER)
S140
키관리서버
(KMA)
S142
키복구서버
(KRA)
S141
데이터
베이스
17

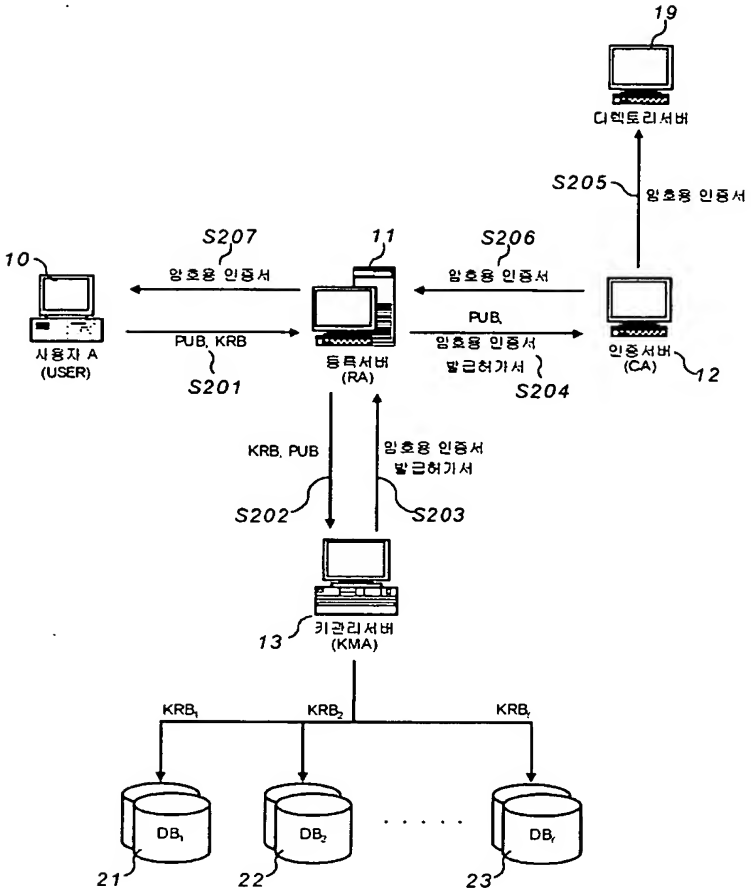
도면3a


10
S154
11
S153
12
사용자 A
(USER)
S150
등록서버
(RA)
S151
인증서버
(CA)
S152
데이터
베이스
17

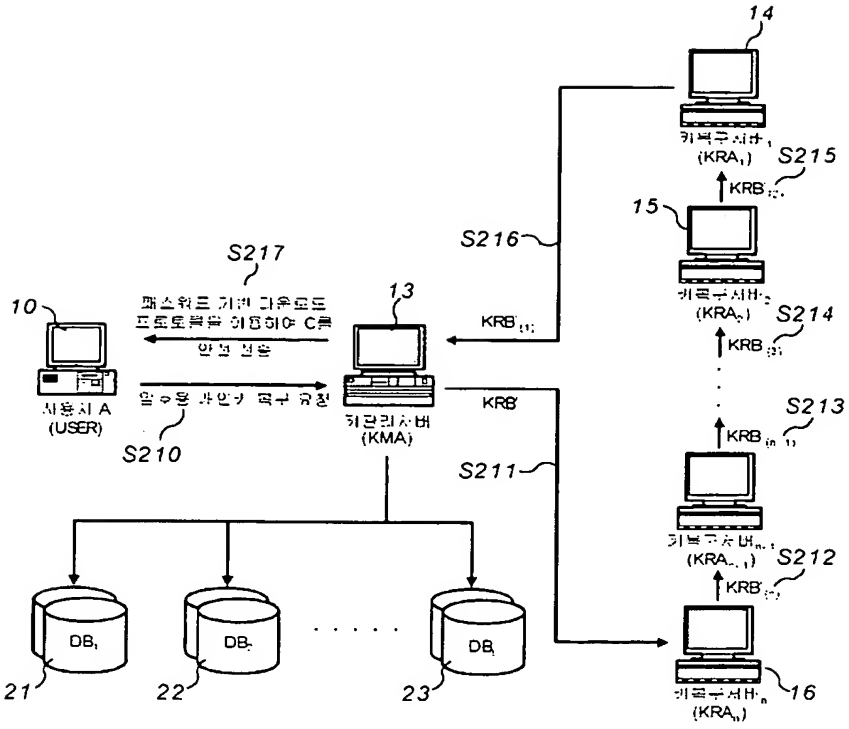
도면3b


10
11
12
S164
S163
S160
S161
S162
사용자 A
(USER)
등록서버
(RA)
인증서버
(CA)
데이터
베이스
17

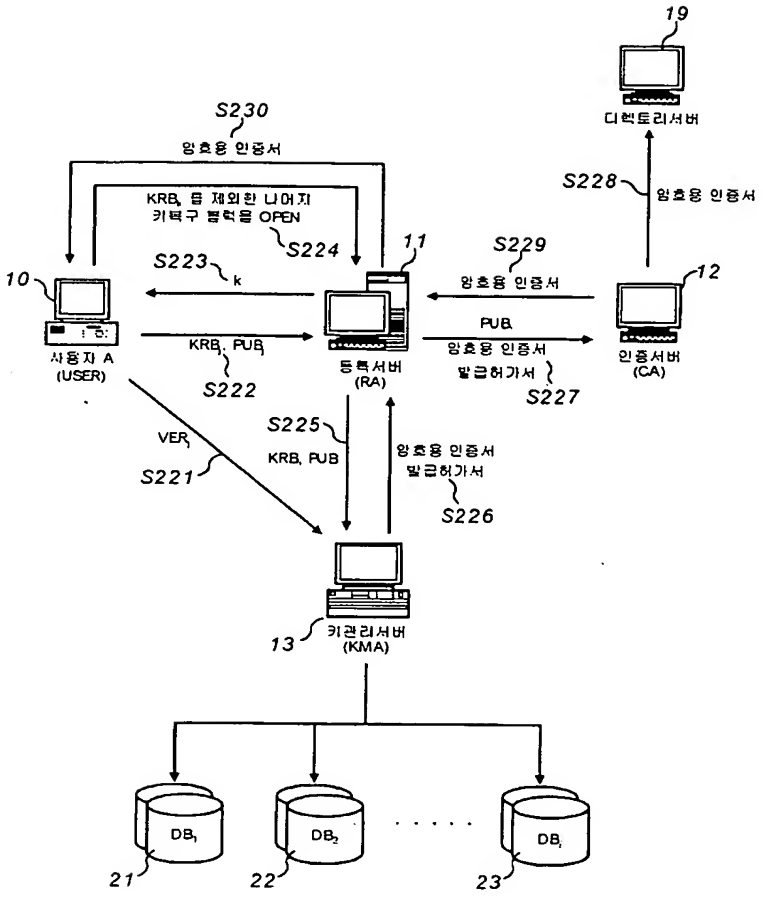
도면4a


19
디렉토리서버
S205
암호용 인증서
S207
암호용 인증서
11
S206
암호용 인증서
10
PUB,
암호용 인증서
발급허가서
S204
사용자 A
(USER)
PUB, KRB
S201
등록서버
(RA)
인증서버
(CA)
12
KRB, PUB
S202
암호용 인증서
발급허가서
S203
13
키관리서버
(KMA)
KRB1
KRB2
KRBr
DB1
DB2
DBr
21
22
23

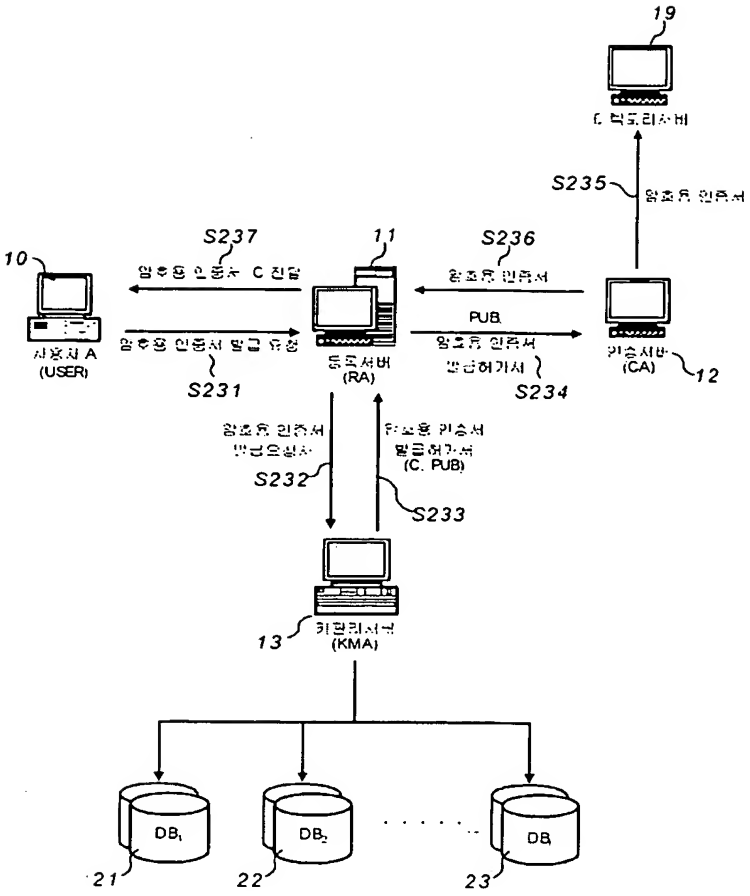
도면4b


14
15
S215
S216
S217
10
13
S214
S213
S211
S212
S210
KRB
DB1
DB2
DBi
21
22
23
16
(KRA1)
(KRA2)
(KRAn)
(USER)
(KMA)

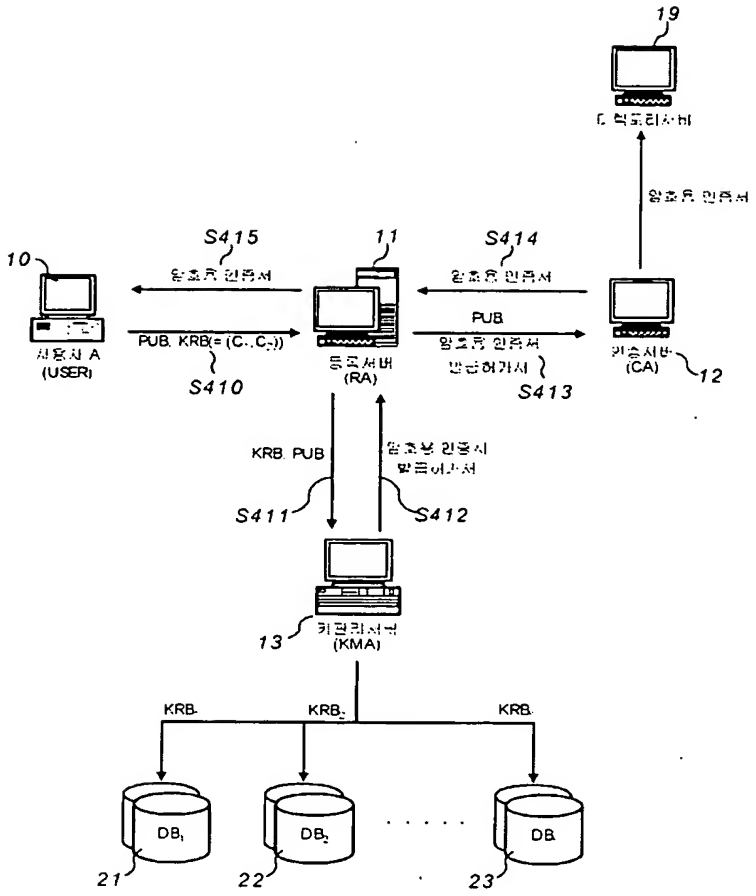
도면5


19
디렉토리서버
S230
암호용 인증서
KRB, 등 제외한 나머지
키복구 블럭을 OPEN
S224
S228
암호용 인증서
11
S229
S223
k
암호용 인증서
12
10
PUB,
KRB, PUB,
암호용 인증서
사용자 A
(USER)
등록서버
(RA)
인증서버
(CA)
발급허가서
S222
S227
S225
VER,
KRB, PUB
암호용 인증서
S221
발급허가서
S226
13
키관리서버
(KMA)
DB1
DB2
DBi
21
22
23

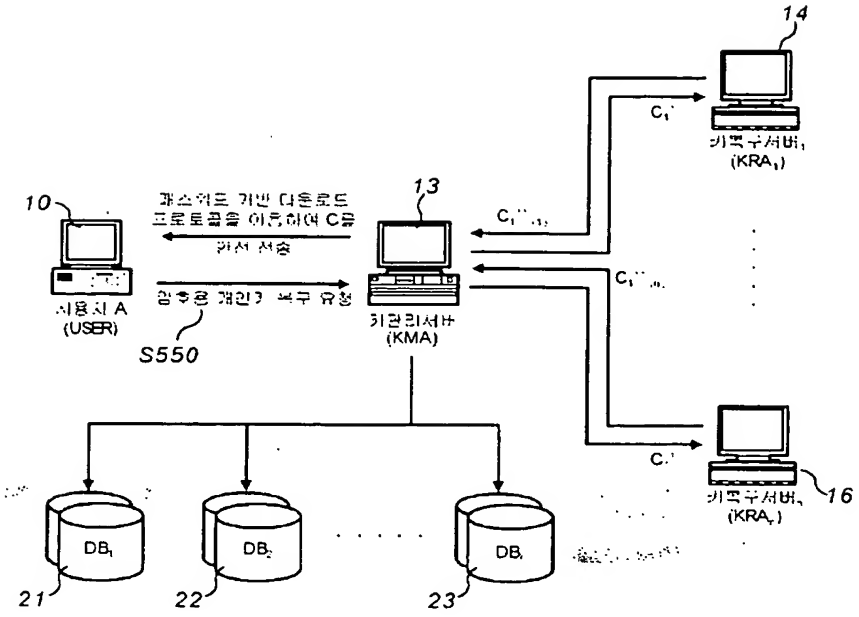
도면6


19
S235
S237
11
S236
10
PUB.
S231
S234
12
S232
S233
13
DB1
DB2
DBn
21
22
23

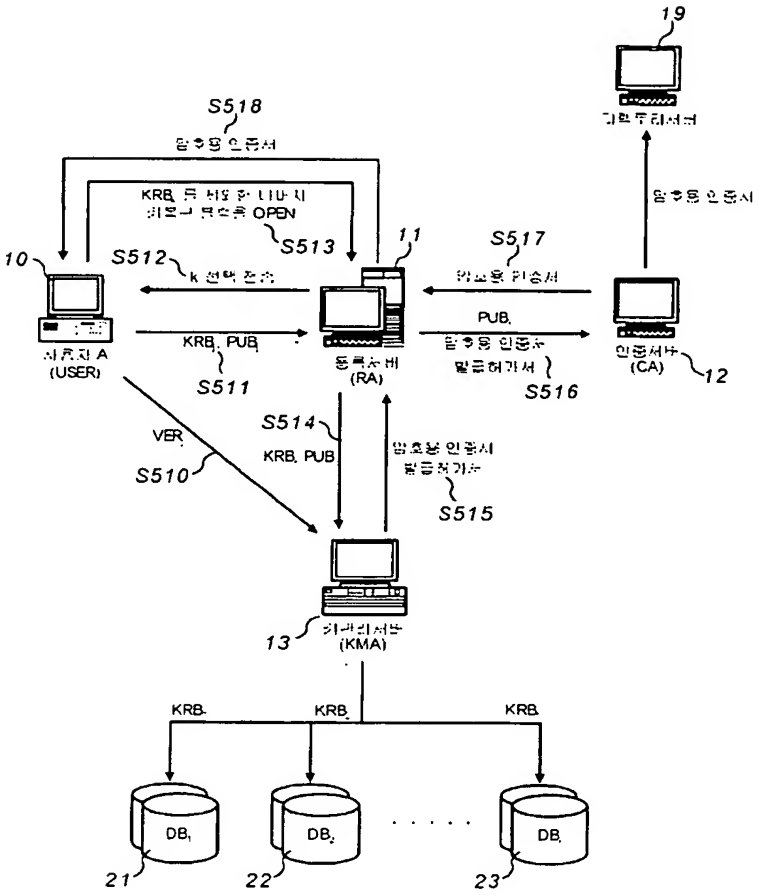
도면7a


19
S415
11
S414
10
PUB, KRB(= (C..C))
S410
등록서버
(RA)
PUB
S413
(CA)
12
KRB, PUB
S411
S412
13
(KMA)
KRB
KRB
KRB
DB
DB
DB
21
22
23

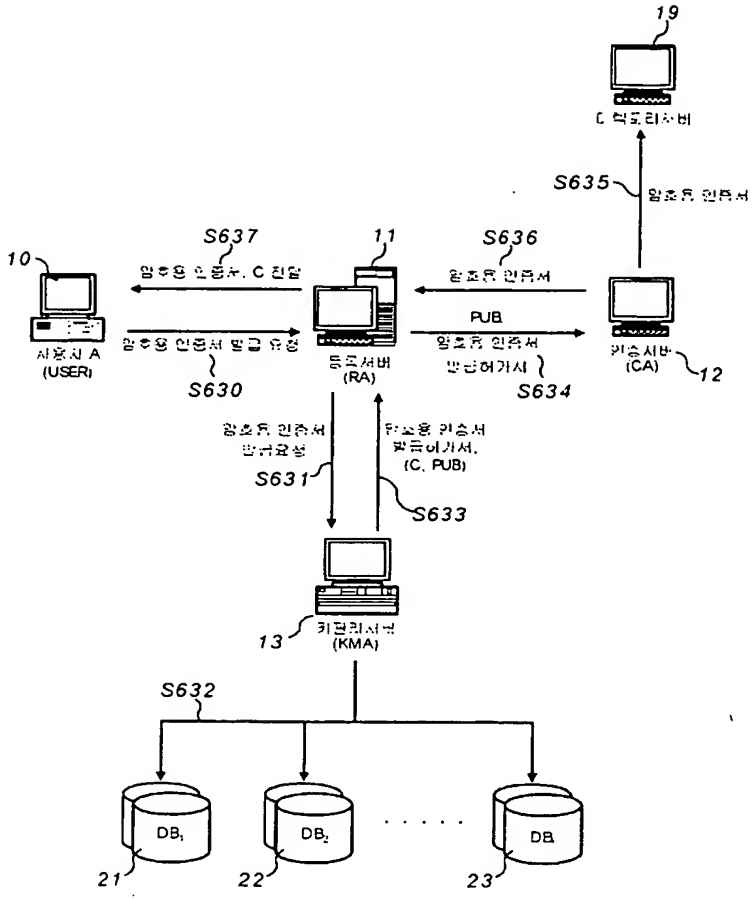
도면7b


14
C_1'
키복구서버$_1$
(KRA_1)
10
13
$C_1''_{(1)}$
패스워드 기반 다운로드
프로토콜을 이용하여 C를
인증서 전송
$C_1''_{(n)}$
사용자 A
(USER)
암호용 개인키 복구 요청
S550
키관리서버
(KMA)
C_n'
키복구서버$_n$
(KRA_n)
16
DB_1
DB_2
DB_i
21
22
23

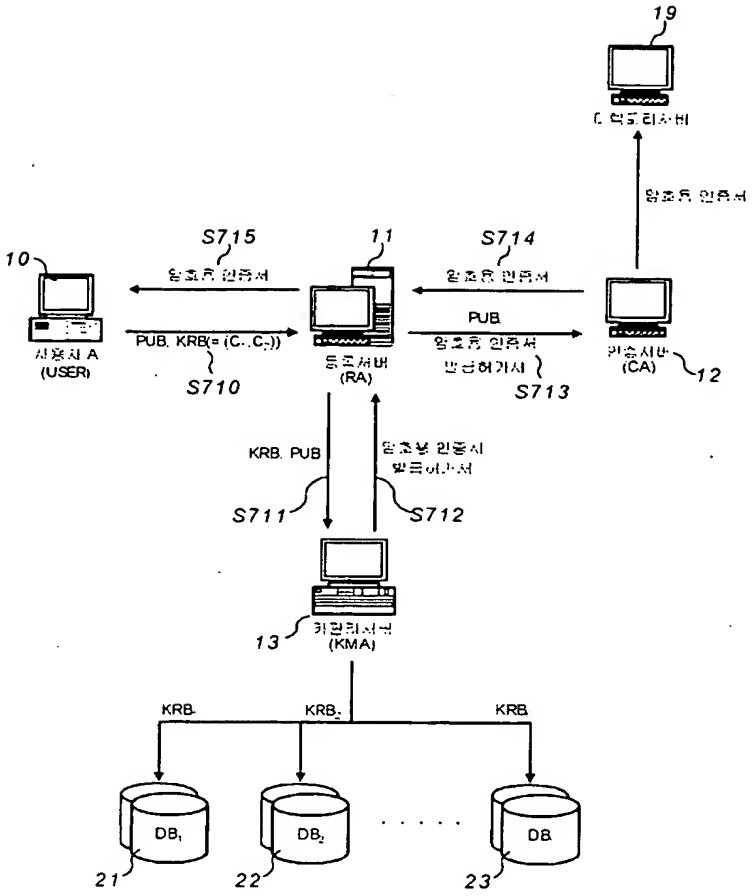
도면8


19
S518
KRB, PUB, OPEN
S513
11
S517
10
S512
KRB, PUB,
S511
PUB,
S516
12
S514
KRB, PUB
VER,
S510
S515
13
KRB,
KRB,
KRB,
DB,
DB,
DB,
21
22
23

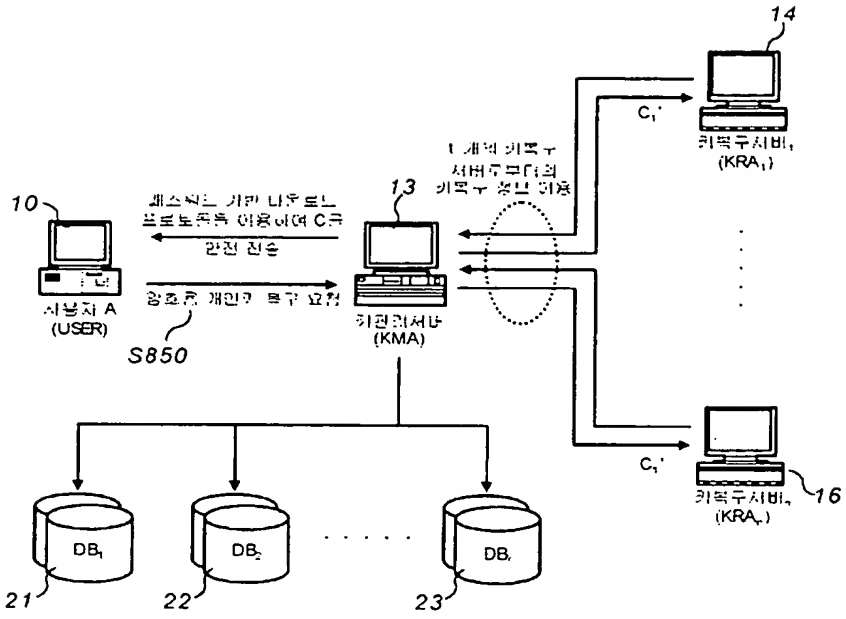
도면9


19
S635
S637
11
S636
10
PUB
S630
S634
12
S631
S633
13
S632
DB1
DB2
DBn
21
22
23

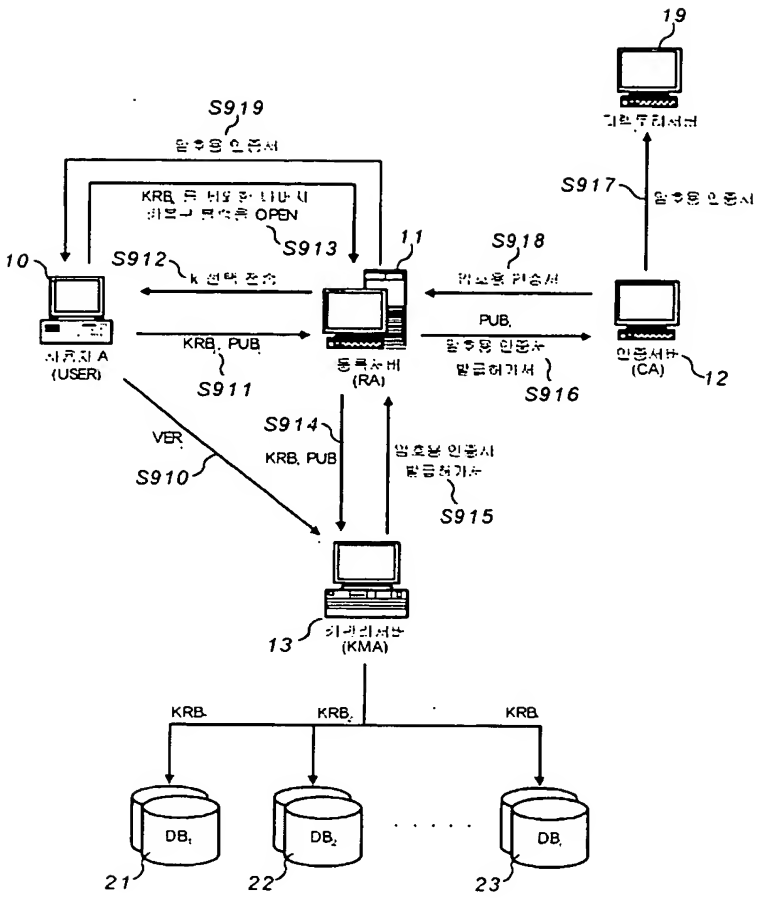
도면10a


19
디렉토리서버
암호화 인증서
S715
11
S714
10
암호화 인증서
암호화 인증서
PUB.
PUB. KRB(= (C...C))
암호화 인증서
사용자 A
(USER)
S710
등록서버
(RA)
발급허가서
S713
인증서버
(CA)
12
KRB. PUB
암호화 인증서
발급허가서
S711
S712
13
키관리서버
(KMA)
KRB
KRB
KRB
DB
DB
DB
21
22
23

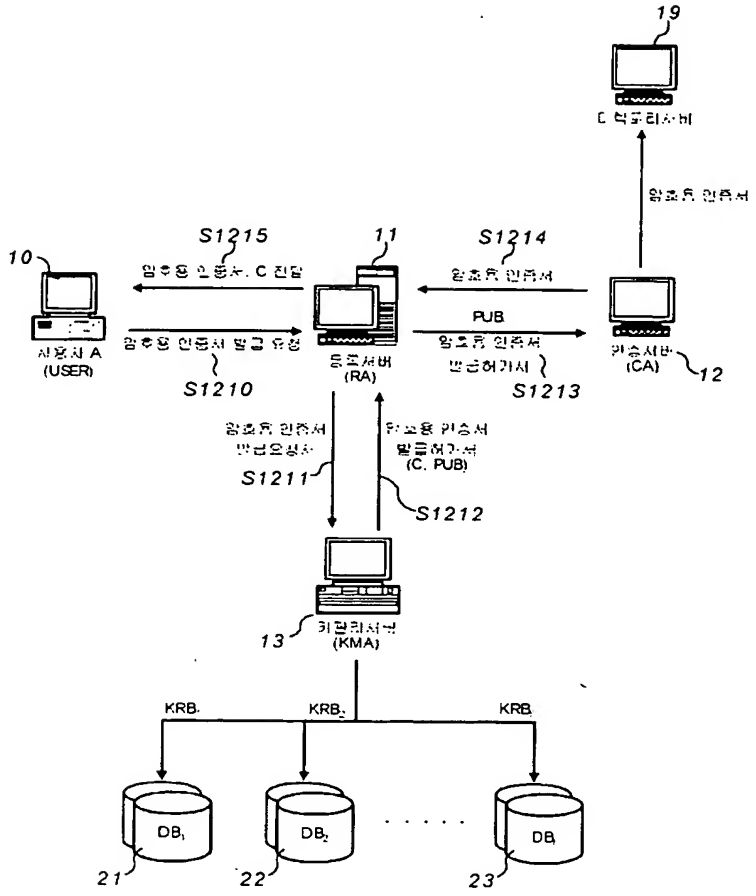
도면10b


14
C1'
키복구서버1
(KRA1)
10
13
사용자 A
(USER)
인증서버
(KMA)
S850
C1'
키복구서버n
(KRAn)
16
DB1
DB2
DBn
21
22
23

도면11


19
S919
S917
S913
S912
11
S918
10
S911
PUB,
S916
12
S914
VER,
S910
KRB, PUB
S915
13
KRB,
KRB,
KRB,
DB,
DB,
DB,
21
22
23

도면12



(57) 청구의 범위

청구항 1

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 생성한 후, 이에 대응되는 패스워드 확인자를 키관리 서버에 등록하는 단계;

(b) 상기 사용자가 자신의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 사용자가 상기 패스워드를 이용하여 상기 개인키를 암호화하는 단계(즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD: 패스워드, PRI: 개인키);

(d) 상기 사용자가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키복구 블럭과 상기 공개키가 키관리 서버에게 전송되는 단계; 및

(f) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 상기 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 2

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 생성한 후, 이에 대응되는 패스워드 확인자를 키관리 서버에 등록하는 단계;

(b) 상기 사용자가 자신의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 사용자가 패스워드를 이용하여 상기 개인키를 암호화하는 단계 (즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD: 패스워드, PRI: 개인키);

(d) 상기 사용자가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키복구 블럭의 정당성을 확인하는 단계;

(f) 정당성이 확인된 키복구 블럭과 개인키와의 대응성이 확인된 공개키가 키관리 서버에게 전송되는 단계; 및

(g) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 3

제2항에 있어서, 상기 키생성 및 위탁 방법은 단계 (c)를 생략하고 단계 (d)에서 사용자가 키복구 서버의 암호용 공개키를 이용하여 사용자의 공개키를 암호화함으로써 키복구 블럭을 생성하는 것을 특징으로 하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 4

(a) PKI 기반의 키위탁 시스템의 키위탁 서비스를 이용하고자 하는 사용자가 자신의 패스워드를 키관리 서버에 등록하는 단계;

(b) 키관리 서버가 상기 사용자의 암호용 개인키와 공개키 쌍을 생성하는 단계;

(c) 상기 키관리 서버가 상기 사용자의 등록된 패스워드를 이용하여 상기 사용자의 개인키를 암호화하는 단계(즉, $C = E_{PWD}(PRI)$를 수행하는 단계 단, PWD; 패스워드, PRI; 개인키);

(d) 상기 키관리 서버가 키복구 서버의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 단계;

(e) 상기 키관리 서버가 키복구 블럭을 저장하거나, 또는 상기 키복구 블럭을 여러 조각으로 분할한 후, 분할된 키복구 블럭 조각을 분산 저장하는 단계

를 포함하는 키위탁 시스템의 키생성 및 위탁 방법.

청구항 5

(a) 키관리 서버가 키복구 요청 메시지를 수신한 후, 위탁된 복구 대상자의 키복구 블럭을 재구성하는 단계;

(b) 상기 키관리 서버가 복수의 키복구 서버 중 어떤 키복구 서버도 키복구 블럭을 풀 수 없도록 하기 위해 자신만이 알고 있는 은닉 인자를 이용하여 키복구 블럭을 은닉하는 단계;

(c) 상기 키관리 서버가 은닉된 키복구 블럭을 암호용 개인키 복구 요청서와 함께 복수의 키복구 서버들에게 전송하는 단계;

(d) 상기 복수의 키복구 서버들이 수신한 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 단계;

(e) 상기 키복구 서버들이 복호화된 메시지를 키관리 서버에게 전송하는 단계;

(f) 상기 키관리 서버가 키복구 서버들로부터 수신한 메시지와 자신만이 알고 있는 은닉 인자를 이용하여 암호화된 사용자의 개인키 C를 복구하는 단계

를 포함하는 키위탁 시스템의 키복구 방법.

청구항 6

제5항에 있어서, 상기 단계 (a)의 키복구 요청은 사용자의 요청 또는 법원으로부터의 요청을 포함하는 키위탁 시스템의 키복구 방법.

청구항 7

제5항에 있어서, 상기 단계 (a)의 키복구 블럭 재구성 단계는 복수의 키복구 블럭 조각 중 일부만으로 키복구 블럭을 재구성하는 것을 포함하는 키위탁 시스템의 키복구 방법.

청구항 8

제5항에 있어서, 상기 단계 (f)의 암호화된 사용자의 개인키 복구 단계는 상기 키관리 서버가 복수의 키복구 서버 중 일부 키복구 서버로부터의 메시지만으로도 상기 암호화된 사용자의 개인키 C를 복구하는 것을 포함하는 키위탁 시스템의 키복구 방법.

청구항 9

제5항에 있어서, 키복구 요청자의 패스워드 확인자를 소지한 상기 키관리 서버가 복구한 암호화된 개인키 C를 패스워드 기반 다운로드 프로토콜을 이용하여 키복구 요청자에게 전송하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 10

제5항에 있어서, 키관리 서버 또는 신뢰 객체가 패스워드에 대한 사전 공격을 통해 C로부터 사용자의 암호용 개인키를 복구하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 11

제5항에 있어서, 키관리 서버 또는 신뢰 객체가 등록되어 있는 사용자의 패스워드를 이용하여 사용자의 암호용 개인키를 복구하는 단계를 포함하는 키위탁 시스템의 키복구 방법.

청구항 12

PKI 기반의 키위탁 시스템의 서비스를 이용하고자, 패스워드를 생성한 후, 그에 대응되는 패스워드 확인자를 키관리 서버에 등록하고 자신의 암호용 개인키와 공개키 쌍을 생성한 후, 상기 패스워드를 이용하여 상기 개인키를 암호화한 $C'(=E_{PWD}(PRI))$ 단, PWD: 패스워드, PRI: 개인키)를 생성하고 키복구 서버들의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성하는 사용자;

상기 키복구 블럭을 저장하거나 키복구 블럭을 여러 조각으로 분할한 키복구 블럭 조각을 분산 저장하며, 키복구 요청을 수신하는 경우, 상기 키복구 블럭을 재구성하고 복수의 키복구 서버 중 어떤 키복구 서버도 재구성된 키복구 블럭을 볼 수 없도록 하기 위해 자신만이 알고있는 은닉 인자를 이용하여 은닉한 키복구 블럭을 암호용 개인키 복구 요청서와 함께 상기 복수의 키복구 서버에게 전송하고, 상기 키복구 서버들로부터 수신한 메시지와 상기 은닉 인자를 이용하여 상기 C를 복구하는 키관리 서버; 및

암호용 개인키 복구 요청서와 함께 수신된 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 키복구 서버

를 포함하는 키위탁 시스템.

청구항 13

제12항에 있어서, 상기 사용자가 생성한 키복구 블럭의 정당성이 확인되는 것을 특징으로 하는 키위탁 시스템.

청구항 14

PKI 기반의 키위탁 시스템의 서비스를 이용하고자, 키관리 서버에 패스워드를 등록하는 사용자;

상기 사용자의 암호용 개인키와 공개키 쌍을 생성한 후, 상기 등록된 패스워드를 이용하여 상기 개인키를 암호화한 $C'(=E_{PWD}(PRI))$ 단, PWD: 패스워드, PRI: 개인키)를 생성하고 키복구 서버들의 암호용 공개키를 이용하여 C를 암호화함으로써 키복구 블럭을 생성한 후, 상기 키복구 블럭을 저장하거나 키복구 블럭을 여러 조각으로 분할한 키복구 블럭 조각을 분산 저장하며, 키복구 요청을 수신하는 경우, 상기 키복구 블럭을 재구성하고 복수의 키복구 서버 중 어떤 키복구 서버도 재구성된 키복구 블럭을 볼 수 없도록 하기 위해 자신만이 알고있는 은닉 인자를 이용하여 은닉한 키복구 블럭을 암호용 개인키 복구 요청서와 함께 상기 복수의 키복구 서버에게 전송하고, 상기 키복구 서버들로부터 수신한 메시지와 상기 은닉 인자를 이용하여 상기 C를 복구하는 키관리 서버; 및

암호용 개인키 복구 요청서와 함께 수신된 메시지에 대해 자신의 개인키를 이용하여 복호화를 수행하는 키복구 서버

를 포함하는 키위탁 시스템.

청구항 15

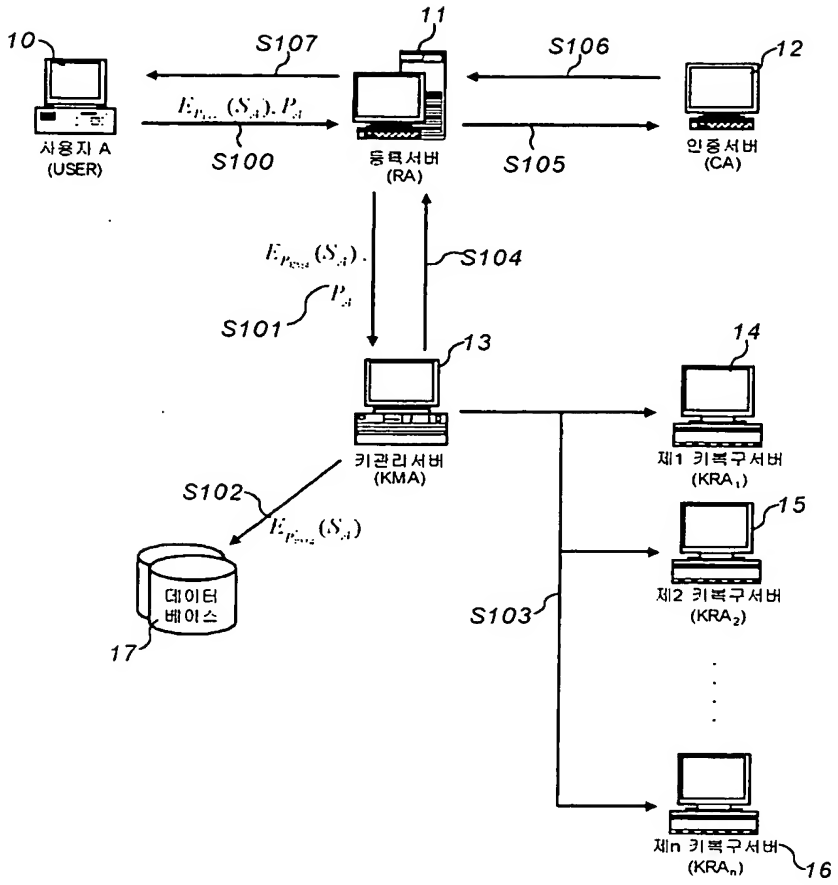
제12항 또는 제14항에 있어서, 복수의 키복구 블럭 조각 중 일부만으로도 키복구 블럭을 재구성하는 키관리 서버를 포함하는 키위탁 시스템.

청구항 16

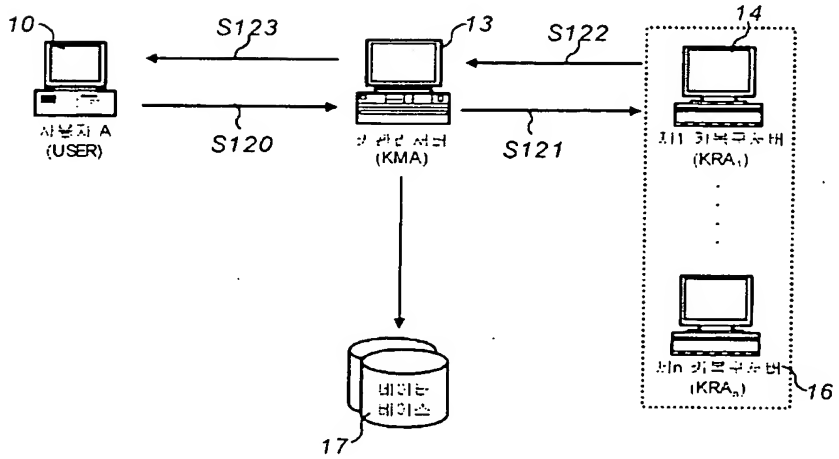
제12항 또는 제14항에 있어서, 복수의 키복구 서버 중 일부 키복구 서버로부터의 메시지만으로도 상기 암호화된 사용자의 개인키 C를 복구하는 키관리 서버를 포함하는 키위탁 시스템.

도면

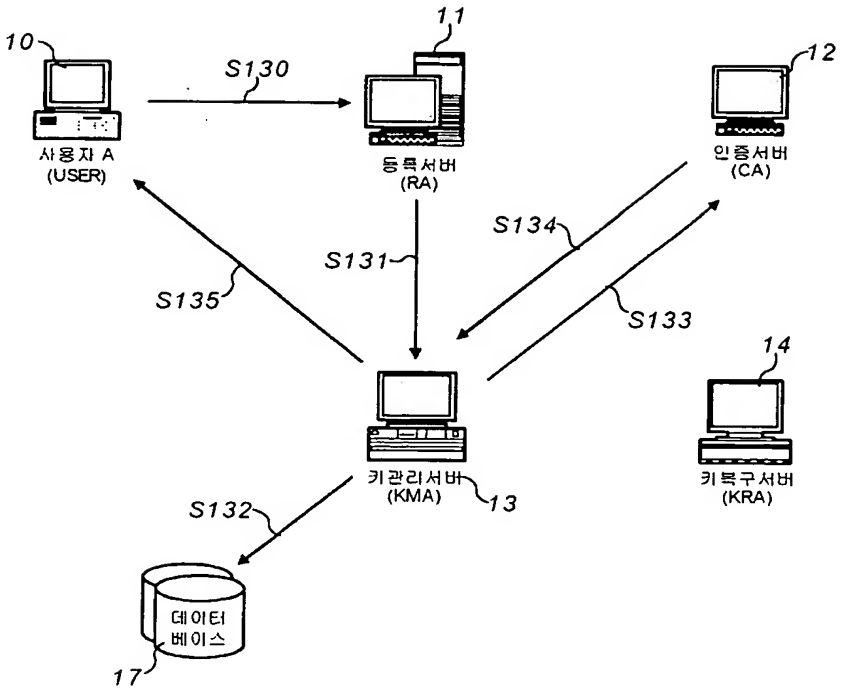
도면1a


10
11
12
S107
S106
$E_{P_{RA}}(S_A), P_A$
S100
S105
사용자 A
(USER)
등록서버
(RA)
인증서버
(CA)
$E_{P_{KMA}}(S_A),$
P_A
S104
S101
13
14
키관리서버
(KMA)
제1 키복구서버
(KRA_1)
S102
$E_{P_{KRA_1}}(S_A)$
15
제2 키복구서버
(KRA_2)
데이터
베이스
S103
17
제n 키복구서버
(KRA_n)
16

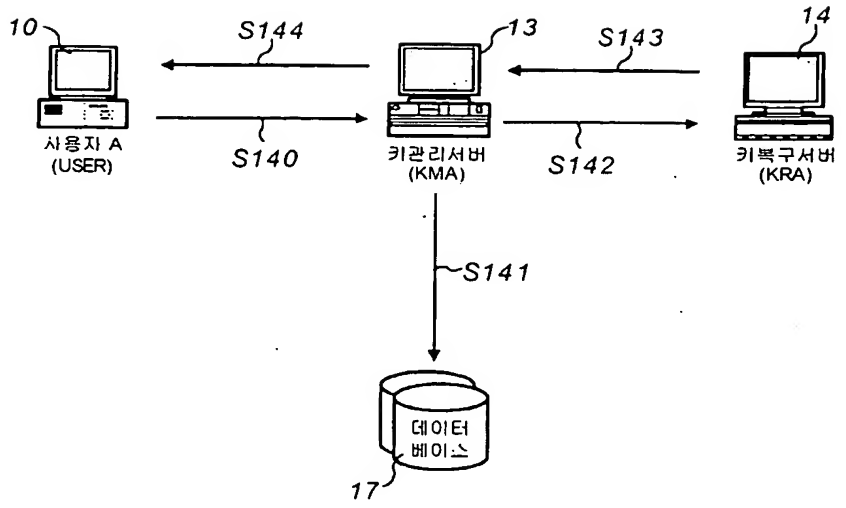
도면1b


10
S123
13
S122
14
사용자 A
(USER)
S120
(KMA)
S121
제1 키복구서버
(KRA_1)
제n 키복구서버
(KRA_n)
16
데이터
베이스
17

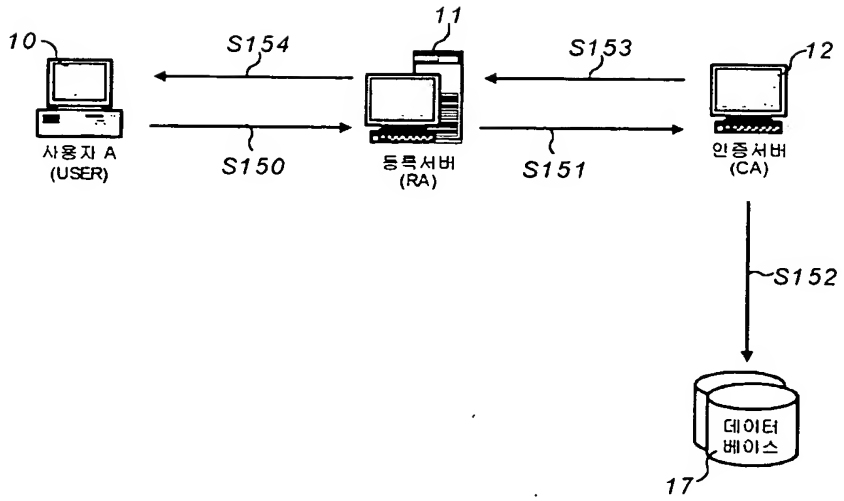
도면2a


10
사용자 A
(USER)
S130
11
등록서버
(RA)
12
인증서버
(CA)
S131
S134
S135
S133
14
키관리서버
(KMA)
13
키복구서버
(KRA)
S132
데이터
베이스
17

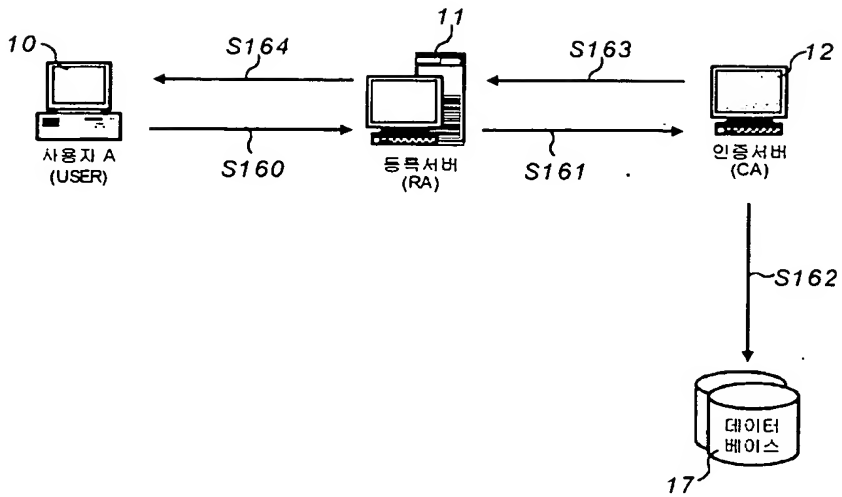
도면2b


10
S144
13
S143
14
사용자 A
(USER)
S140
키관리서버
(KMA)
S142
키복구서버
(KRA)
S141
데이터
베이스
17

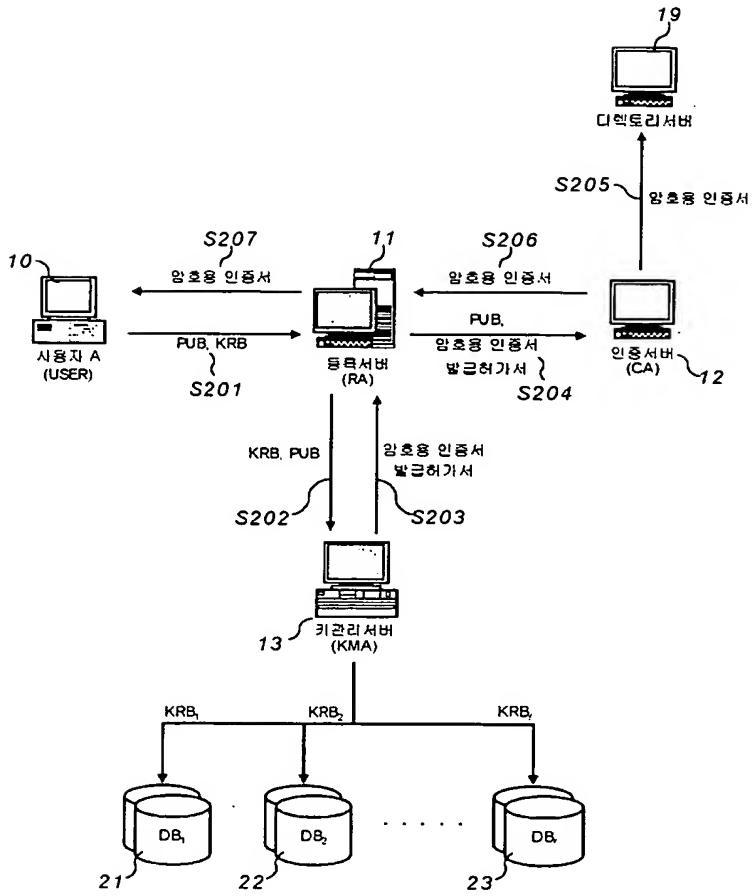
도면3a


10
S154
11
S153
12
사용자 A
(USER)
S150
등록서버
(RA)
S151
인증서버
(CA)
S152
데이터
베이스
17

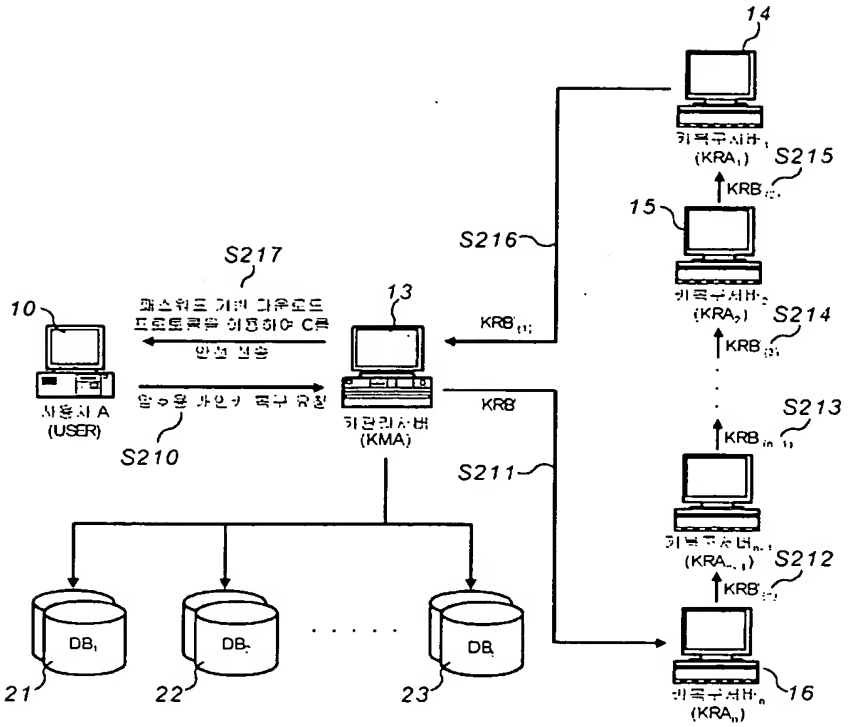
도면3b


10
사용자 A
(USER)
S164
S160
11
등록서버
(RA)
S163
S161
12
인증서버
(CA)
S162
데이터
베이스
17

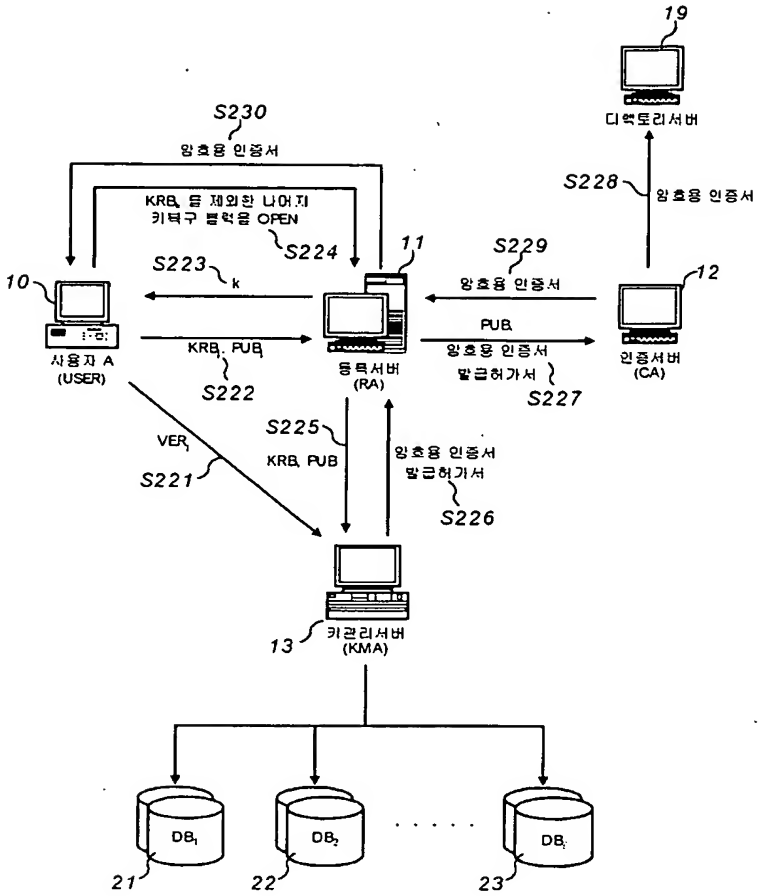
도면4a


19
디렉토리서버
S205
암호용 인증서
S207
암호용 인증서
11
S206
암호용 인증서
10
PUB,
암호용 인증서
PUB, KRB
발급허가서
S204
S201
등록서버
(RA)
인증서버
(CA)
12
사용자 A
(USER)
KRB, PUB
암호용 인증서
발급허가서
S202
S203
13
키관리서버
(KMA)
KRB1
KRB2
KRBn
DB1
DB2
DBn
21
22
23

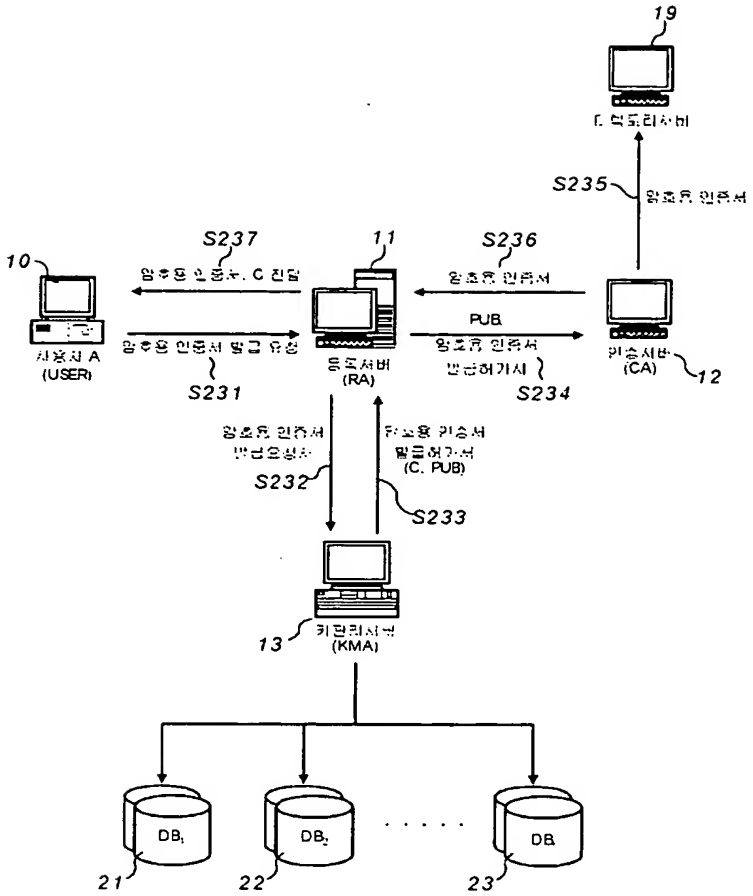
도면4b


14
15
16
13
10
S210
S211
S212
S213
S214
S215
S216
S217
KRB
DB1
DB2
DB
21
22
23
(KMA)
(USER)

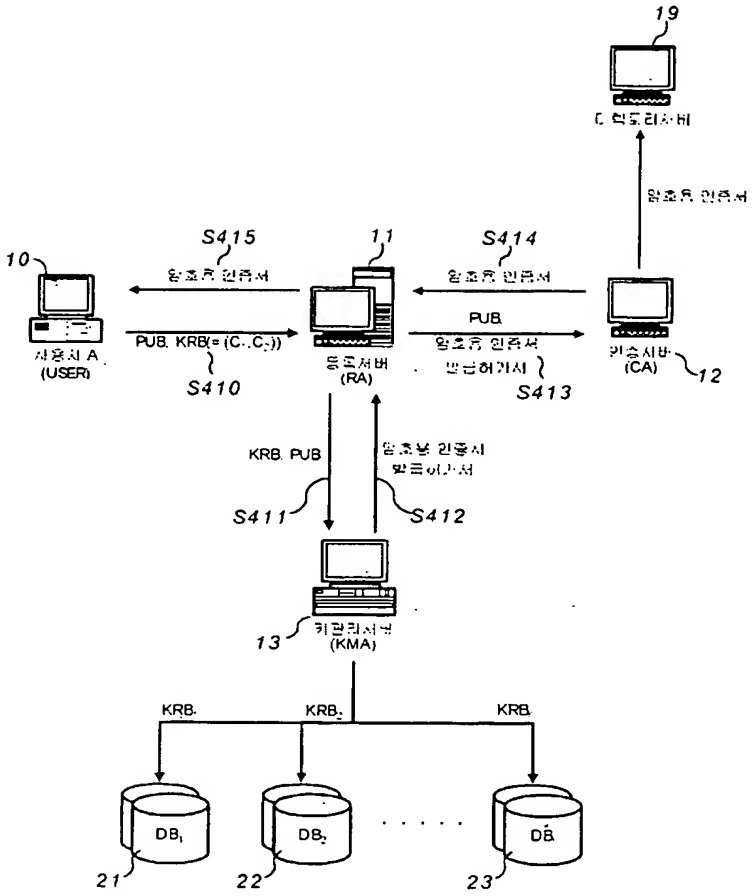
도면5


19
디렉토리서버
S230
암호용 인증서
KRB, 등 제외한 나머지
키복구 블럭을 OPEN
S224
S228
암호용 인증서
11
S229
암호용 인증서
12
10
S223
k
PUB,
암호용 인증서
발급허가서
S227
사용자 A
(USER)
KRB, PUB,
S222
등록서버
(RA)
인증서버
(CA)
S225
VER,
KRB, PUB
S221
암호용 인증서
발급허가서
S226
13
키관리서버
(KMA)
DB1
DB2
DBi
21
22
23

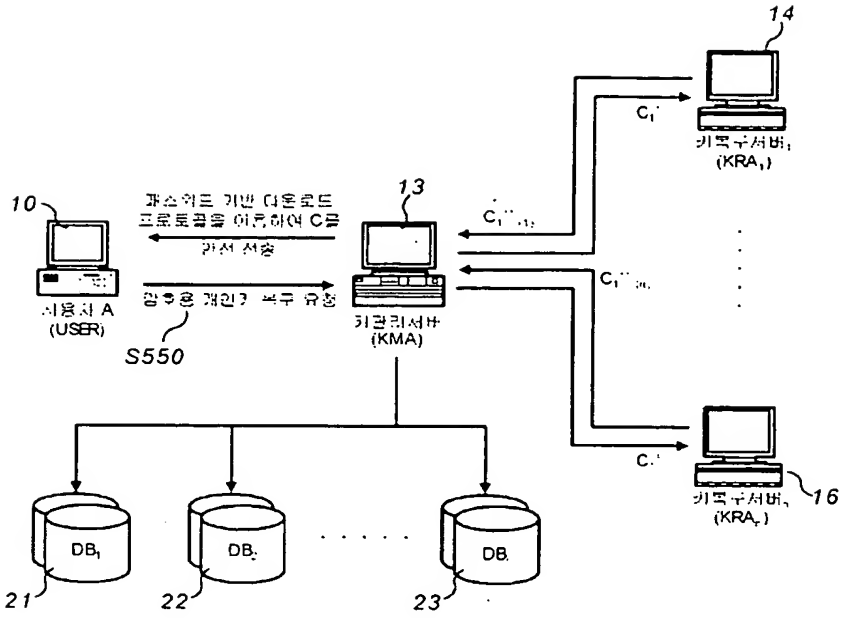
도면6


19
S235
S237
11
S236
10
PUB.
S231
S234
S232
S233
13
(KMA)
DB1
DB2
DBn
21
22
23

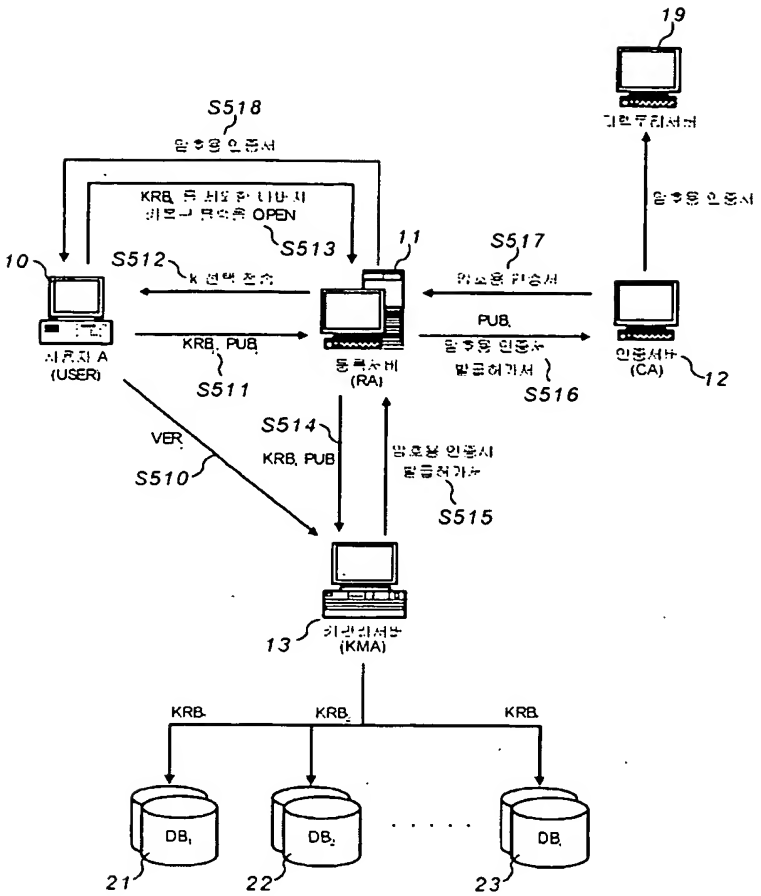
도면7a


19
S415
11
S414
10
PUB. KRB(= (C., C.))
S410
PUB.
S413
12
KRB. PUB
S411
S412
13
KRB.
KRB.
KRB.
DB.
DB.
DB.
21
22
23

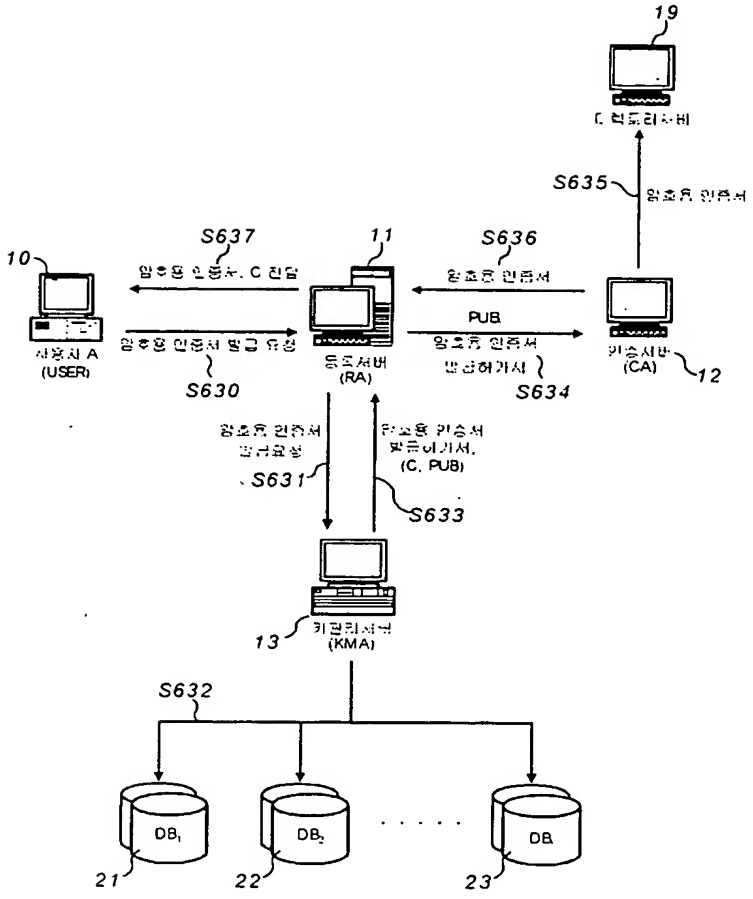
도면7b



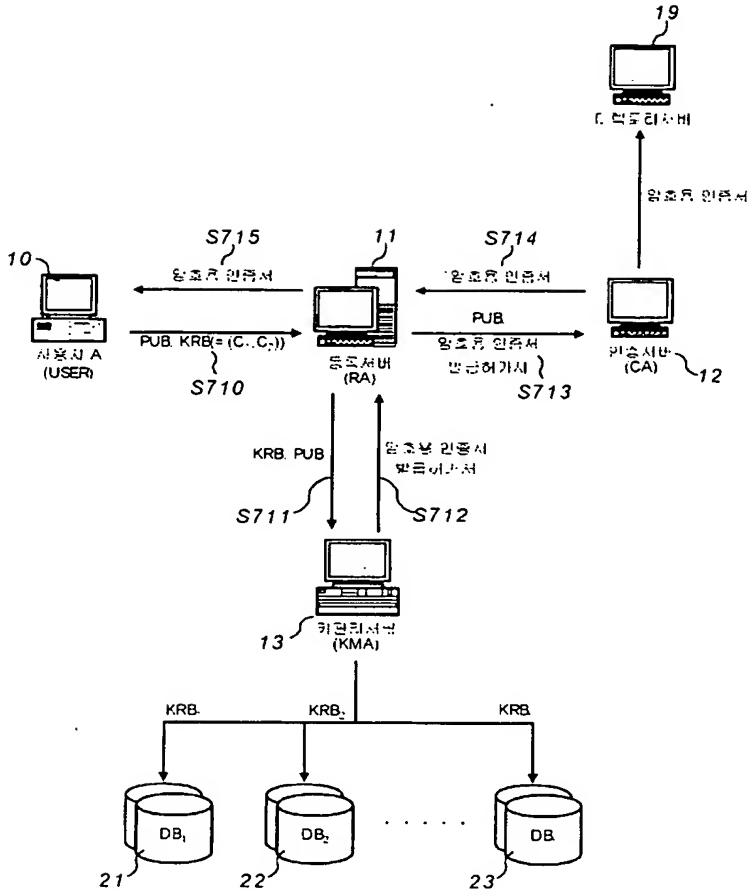
도면8


19
S518
KRB, PUB
S513
11
S517
S512
10
PUB
KRB, PUB
S511
S516
12
S514
VER
KRB, PUB
S510
S515
13
KRB
KRB
KRB
DB
DB
DB
21
22
23

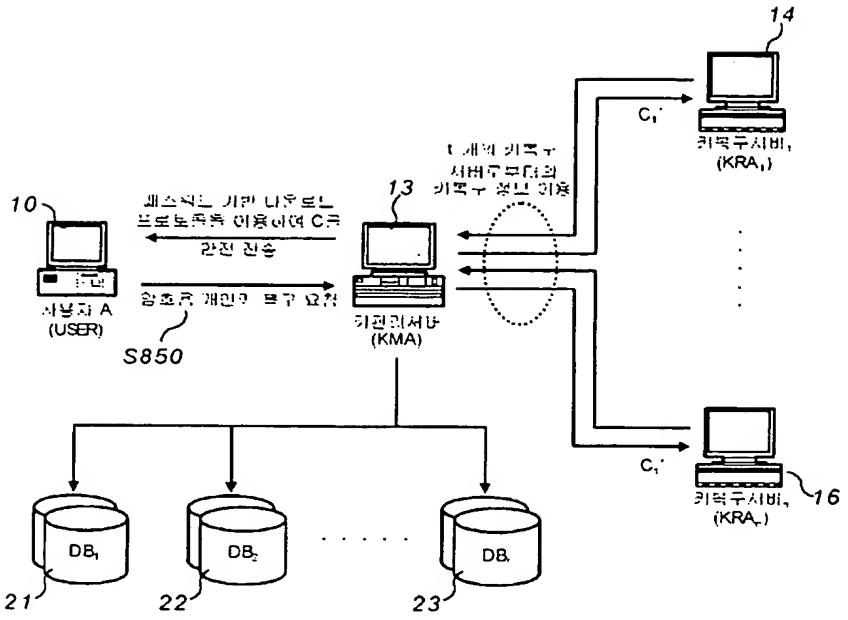
도면9


19
S635
10
S637
11
S636
PUB
S630
S634
S631
S633
13
S632
DB1
DB2
DBn
21
22
23
12

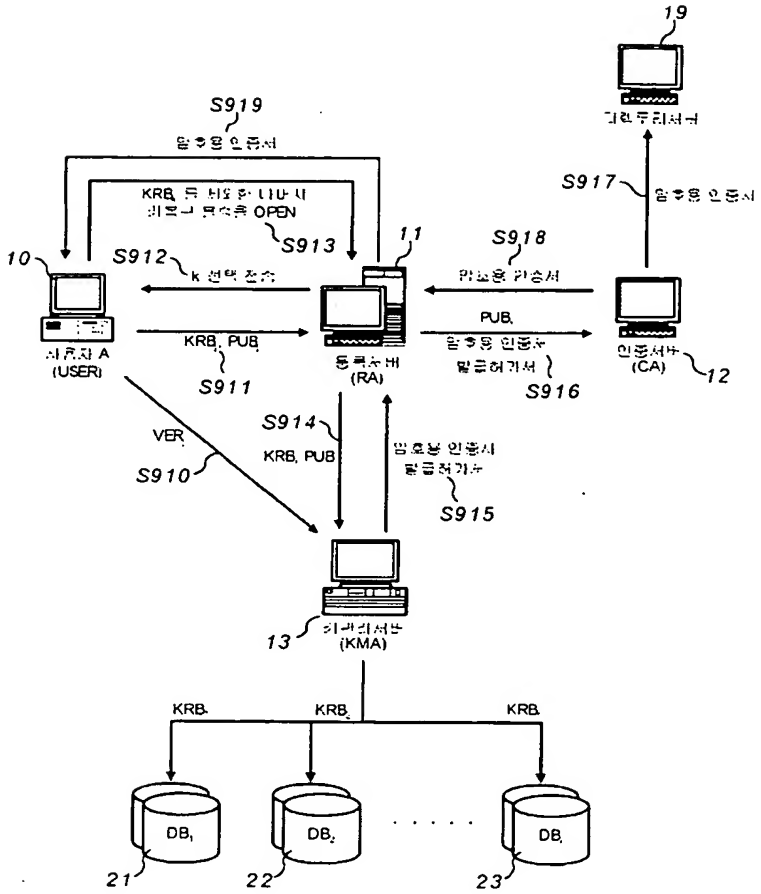
도면10a


19
S715
11
S714
10
PUB, KRB(= (C, C))
S710
PUB
S713
12
KRB, PUB
S711
S712
13
KRB
KRB
KRB
DB
DB
DB
21
22
23

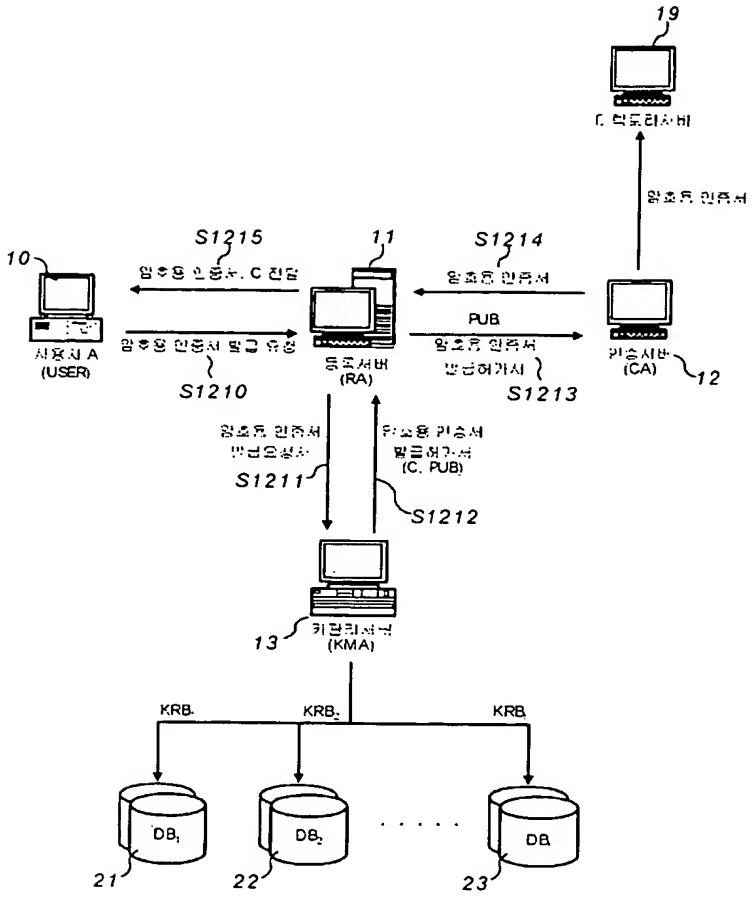
도면10b


14
C1'
키복구서버1
(KRA1)
10
13
사용자 A
(USER)
인증서버
(KMA)
S850
Cn'
키복구서버n
(KRAn)
16
DB1
DB2
DBn
21
22
23

도면11


19
S919
S917
S913
11
S918
10
S912
S911
S914
VER
S910
KRB, PUB
S915
S916
12
13
KRB
KRB
KRB
DB1
DB2
DBi
21
22
23

도면12


19
C 인증디렉토리서버
인증서 인증서
S1215
11
S1214
10
인증서 C 전달
인증서 인증서
PUB
사용자 A
(USER)
인증서 발급 요청
등록서버
(RA)
인증서
발급허가서
인증서
(CA)
12
S1210
S1213
인증서
발급요청서
S1211
S1212
(C. PUB)
13
(KMA)
KRB.
KRB.
KRB.
DB.
DB.
DB.
21
22
23